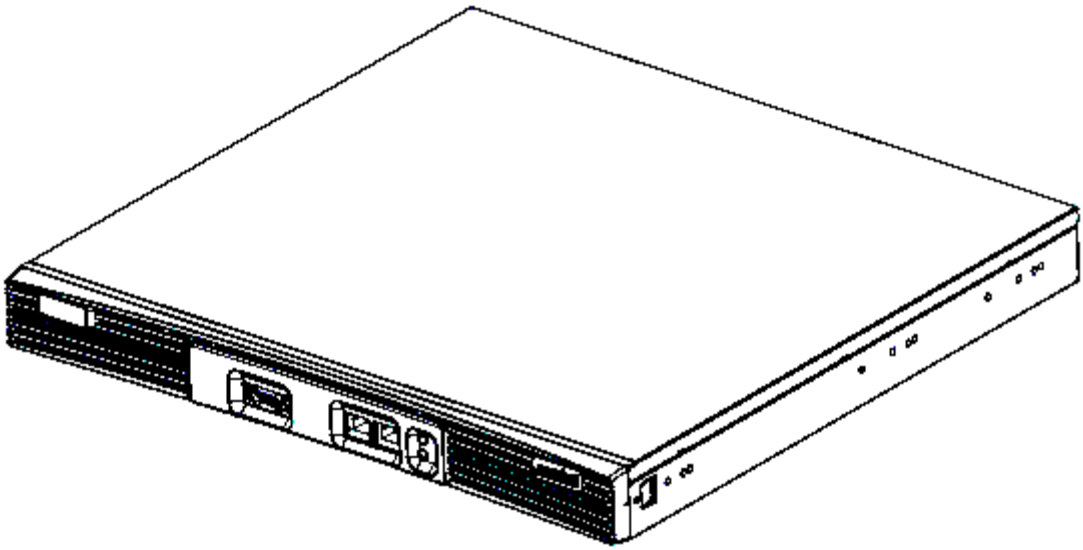
WS5100 Series Switch

CLI REFERENCE GUIDE



symbol®
The Enterprise Mobility Company™

Contents

About This Guide

Chapter 1. Introduction

CLI Overview 1-1
Getting Context Sensitive Help 1-4
Using the no and default Forms of Commands 1-6
Using History Command 1-7
- Setting the History Command Buffer Size 1-7
- Recalling Commands 1-7
- Disabling the History Command Feature 1-8
- Basic Conventions. 1-8

Using CLI Editing Features and Shortcuts 1-9
- Moving the Cursor on the Command Line 1-9
- Completing a Partial Command Name 1-10
- Deleting Entries 1-11
- Re-displaying the Current Command Line 1-11
- Command Output pagination 1-12

Transposing Mistyped Characters 1-12
Controlling Capitalization 1-12

Chapter 2. Common Commands

Common Commands 2-2
clrscr 2-3
exit 2-4
help 2-5
no 2-7
service 2-8
terminal 2-19
show 2-20
autoinstall 2-22
banner 2-23
commands 2-24
crypto 2-25
environment 2-28
history 2-29
interfaces 2-30
ip 2-32
ldap 2-38
licenses 2-40
logging 2-41
mac 2-42
management 2-43
mobility 2-44
ntp 2-47
privilege 2-49
radius 2-50
redundancy-group 2-51
redundancy-history 2-53
redundancy-members 2-54
snmp 2-55
snmp-server 2-56
terminal 2-59
timezone 2-60
users 2-61

version 2-62
wireless 2-63
access-list 2-70
alarm-log 2-71
boot 2-72
clock 2-73
debugging 2-74
file 2-75
ftp 2-76
password-encryption 2-77
running-config 2-78
securitymgr 2-81
sessions 2-82
startup-config 2-83
upgrade-status 2-84

Chapter 3. User Exec Commands

User Exec Commands 3-2
autoinstall 3-3
clear 3-4
cluster-cli 3-6
debug 3-7
disable 3-9
enable 3-10
logout 3-11
page 3-12
quit 3-13

Chapter 4. Privileged Exec Commands

Priv Exec Command 4-2
acknowledge 4-4
archive 4-5
autoinstall 4-7
cd 4-8
clear 4-9
clock 4-11
cluster-cli 4-12

configure 4-13
copy 4-14
debug 4-15
delete 4-16
diff 4-17
dir 4-18
disable 4-19
edit 4-20
enable 4-22
erase 4-23
halt 4-24
kill 4-25
logout 4-26
mkdir 4-27
more 4-28
page 4-30
ping 4-31
pwd 4-32
quit 4-33
reload 4-34
rename 4-35
rmdir 4-36
telnet 4-37
traceroute 4-38
upgrade 4-39
upgrade-abort 4-41
write 4-42

Chapter 5. Global Configuration Commands

Global Configuration Commands 5-2
aaa 5-4
access-list 5-5
banner 5-6
boot 5-7
country-code 5-8
crypto 5-11
do 5-16

end 5-17
fallback 5-18
ftp 5-19
hostname 5-20
interface 5-21
ip 5-22
license 5-26
line 5-27
local 5-28
logging 5-29
mac 5-31
ntp 5-32
prompt 5-36
radius-server 5-37
redundancy 5-39
service 5-41
snmp-server 5-43
terminal 5-50
timezone 5-51
username 5-52
vpn 5-53
wireless 5-54

Chapter 6. crypto-isakmp

Crypto Isakmp Config commands 6-1
authentication 6-3
clrscr 6-4
encryption 6-5
end 6-6
exit 6-7
group 6-8
hash 6-9
help 6-10
lifetime 6-11
no 6-12
service 6-13
show 6-14

Chapter 7. crypto-group

Crypto Client Config commands 7-1
clrscr 7-3
dns 7-4
end 7-5
exit 7-6
help 7-7
service 7-8
show 7-9
wins 7-11

Chapter 8. crypto-peer

Crypto Peer Config commands 8-1
clrscr 8-3
end 8-4
exit 8-5
help 8-6
no 8-7
service 8-8
set 8-9
show 8-10

Chapter 9. crypto-ipsec

Crypto Ipsec Config commands 9-1
mode 9-3
show 9-4

Chapter 10. crypto-map

Trustpoint Config commands 10-1
clrscr 10-3
end 10-4
exit 10-5
help 10-6
match 10-7
no 10-9
service 10-10

set 10-11
show 10-14

Chapter 11. crypto-trustpoint Instance

Trustpoint Config commands 11-1
clrscr 11-3
company-name 11-4
email 11-5
end 11-6
exit 11-7
fqdn 11-8
help 11-9
ip-address 11-10
no 11-11
password 11-12
rsakeypair 11-13
service 11-14
show 11-16
subject-name 11-18

Chapter 12. interface Instance

Interface Config commands 12-1
clrscr 12-3
crypto 12-4
description 12-5
duplex 12-6
end 12-7
exit 12-8
help 12-9
ip 12-10
management 12-11
mtu 12-12
no 12-13
service 12-14
show 12-17
shutdown 12-20
speed 12-21

switchport 12-22
terminal 12-24
tunnel 12-25

Chapter 13. Extended ACL Instance

Extended ACL Config Commands 13-1
clrscr 13-3
deny 13-4
end 13-6
exit 13-7
help 13-8
mark 13-9
no 13-11
permit 13-12
service 13-14
show 13-16
terminal 13-18

Chapter 14. Standard ACL Instance

Standard ACL Config Commands 14-1
clrscr 14-3
deny 14-4
end 14-5
exit 14-6
help 14-7
mark 14-8
no 14-9
permit 14-10
service 14-11
show 14-13
terminal 14-15

Chapter 15. Extended MAC ACL Instance

MAC Extended ACL Config Commands 15-1
clrscr 15-3
deny 15-4
end 15-6

exit 15-7
help 15-8
mark 15-9
no 15-11
permit 15-12
service 15-13
show 15-15
terminal 15-17

Chapter 16. Radius Server Instance

Radius Configuration Commands 16-1
authentication 16-3
ca 16-4
clrscr 16-5
crl-check 16-6
end 16-7
exit 16-8
group 16-9
clrscr 16-10
end 16-10
exit 16-11
group 16-11
guest-group 16-12
help 16-12
no 16-13
policy 16-14
rad-user 16-15
service 16-16
show 16-16
terminal 16-18
Example–Creating a Group 16-19
help 16-21
ldap-server 16-22
nas 16-23
no 16-24
proxy 16-25

rad-user 16-27
server 16-28
service 16-29
show 16-30
terminal 16-32

Chapter 17. Wireless Instance

Wireless Configuration Commands 17-1
adopt-unconf-radio 17-4
adoption-pref-id 17-5
ap-detection 17-6
broadcast-tx-speed 17-8
clrscr 17-9
convert-ap 17-10
country-code 17-11
dhcp-sniff-state 17-14
dot11-shared-key-auth 17-15
end 17-16
exit 17-17
fix-windows-dhcp 17-18
help 17-19
ids 17-20
mac-auth-local 17-22
manual-wlan-mapping 17-23
mobility 17-24
no 17-25
oversized-frames 17-26
proxy-arp 17-27
qos-mapping 17-28
radio 17-29
self-heal 17-36
sensor 17-38
service 17-39
show 17-42
smart-scan-channels 17-44
terminal 17-45
wlan 17-46

About This Guide

This preface introduces the *WS5100 Series CLI Reference Guide* and contains the following sections:

- *Who Should Use this Guide*
- *How to Use this Guide*
- *Conventions Used in this Guide*
- *Service Information*

Who Should Use this Guide

The *WS5100 Series CLI Reference Guide* is intended for system administrators responsible for the implementing, configuring, and maintaining the WS5100 Series Switch within the wireless local area network. It also serves as a reference for configuring and modifying most common system settings. The administrator should be familiar with wireless technologies, network concepts, ethernet concepts, as well as IP addressing and SNMP concepts.

How to Use this Guide

This guide will help you implement, configure, and administer the WS5100 Series Switch and associated network elements. This guide is organized into the following sections:

Table 1 Quick Reference on How This Guide Is Organized

Chapter	Jump to this section if you want to...
Chapter 1, "Introduction"	Review the overall feature-set of the WS5100 Series Wireless Switch, as well as the many configuration options available.
Chapter 2, "Common Commands"	Summarizes the commands common amongst many contexts and instance contexts within the WS5100 Series Wireless Switch command line interface.
Chapter 3, "User Exec Commands"	Summarizes the User Exec commands within the WS5100 Series Wireless Switch command line interface.
Chapter 4, "Privileged Exec Commands"	Summarizes the Priv Exec commands within the WS5100 Series Wireless Switch command line interface.
Chapter 5, "Global Configuration Commands"	Summarizes the Global Config commands within the WS5100 Series Wireless Switch command line interface.
Chapter 6, "crypto-isakmp"	Summarizes the **`crypto-isakmp`** commands within the WS5100 Series Switch command line interface
Chapter 7, "crypto-group"	Summarizes the **`crypto-group`** commands within the WS5100 Series Switch command line interface
Chapter 8, "crypto-peer"	Summarizes the **`crypto-peer`** commands within the WS5100 Series Switch command line interface
Chapter 9, "crypto-ipsec"	Summarizes the **`crypto-ipsec`** commands within the WS5100 Series Switch command line interface
Chapter 10, "crypto-map"	Summarizes the **`crypto-map`** commands within the WS5100 Series Switch command line interface
Chapter 11, "crypto-trustpoint Instance"	Summarizes the **`crypto trustpoint`** commands within the WS5100 Series Wireless Switch command line interface
Chapter 12, "interface Instance"	Summarizes the **`config-if`** commands within the WS5100 Series Wireless Switch command line interface.

Table 1 Quick Reference on How This Guide Is Organized (Continued)

Chapter	Jump to this section if you want to...
Chapter 13, "Extended ACL Instance"	Summarizes the **`config-ext-nacl`** commands within the WS5100 Series Switch command line
Chapter 14, "Standard ACL Instance"	Summarizes the **`config-std-nacl`** commands within the WS5100 Series Switch command line
Chapter 15, "Extended MAC ACL Instance"	Summarizes the **`config-ext-macl`** commands within the WS5100 Series Switch command line
Chapter 16, "Radius Server Instance"	Summarizes the **`(config-radsrv)`**instance commands within the WS5100 Series Wireless Switch command line interface
Chapter 17, "Wireless Instance"	Summarizes the **`(config-wireless)`**instance commands within the WS5100 Series Wireless Switch command line interface.

Conventions Used in this Guide

This section describes the following topics:

- *Annotated Symbols*
- *Notational Conventions*

Annotated Symbols

The following document conventions are used in this document:

NOTE Indicate tips or special requirements.

CAUTION Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Table 1-1. Notational Convention used in the document

Convention	Example Token	Description	Valid Inputs
bold		Bold text indicates commands and keywords that you enter literally	
italics		Italic text indicates arguments for which you supply values.	
()	(on|off)	Grouping (exactly one of a list of tokens)	on
{}	{key1|key2|key3}	Selective recursive (multiple tokens allowed, but each can only be used once)	key1 key3
[ ]	[key1|key2|key3]	Infinite recursive (multiple tokens allowed, each can be used multiple times)	key1 key1 key2 key3 key2 key3
.	.<1-10>	Simple infinite recursive	1 2 6
?	[key1|?key2]	Selective keyword in infinite recursive (multiple tokens, but you can pick one that's only allowed once)	key1 key1 key2

Service Information

Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- serial number of unit
- model number or product name
- software type and version number

North American Contacts

Inside North America:

Symbol Technologies, Inc.

One Symbol Plaza Holtsville, New York 11742-1300

Telephone: 1-631-738-2400/1-800-SCAN 234

Fax: 1-631-738-5990

Symbol Support Center (for warranty and service information):

telephone: 1-800-653-5350

fax: (631) 738-5410

Email: *support@symbol.com*

International Contacts

Outside North America:

Symbol Technologies
Symbol Place
Winnersh Triangle, Berkshire, RG41 5TP
United Kingdom
0800-328-2424 (Inside UK)
+44 118 945 7529 (Outside UK)

Web Support Sites

MySymbolCare

http://www.symbol.com/services/msc/msc.html

Symbol Services Homepage

http://symbol.com/services

Symbol WS5100 Manuals

http://www.symbol.com/legacy_manuals/wire/ws5100.html

Symbol Developer Program

http://devzone.symbol.com

Additional Information

Obtain additional information by contacting Symbol at:

1-800-722-6234, inside North America
+1-516-738-5200, in/outside North America
http://symbol.com/

1

Introduction

This chapter describes the commands that are defined by the WS5100 Series Command Line Interface (CLI). Access the CLI by running a terminal emulation program on a computer that is connected to the serial port at the front of the switch, or by using Telnet via secure shell (SSH) to access the switch over the network.

The default cli user is **cli**. The default username and password is admin and superuser, respectively.

1.1 CLI Overview

The Symbol command-line interface (CLI) is used for configuring, monitoring, and maintaining Symbol devices. This user interface allows you to execute commands, whether using a serial console or using remote access methods.

This chapter describes the basic features of the Symbol CLI's and how to use them. Topics covered include an introduction to Symbol command modes, navigation and editing features, help features, and command history features.

To aid in the configuration of Symbol devices, the Symbol CLI is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring. The commands available to you at any given time depend on the mode you are in. Enter a question mark (**?**) at the system prompt to view the list of commands available for each command mode/instance.

The use of specific commands allows you to navigate from one command mode to another. The standard order that a user would access the modes is as follows: USER EXEC mode; PRIV EXEC mode and GLOBAL CONFIG mode.

When you start a session on a switch, you generally begin in USER EXEC mode, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in USER EXEC mode. This level of access is reserved for tasks that do not change the configuration of the switch, such as determining the current switch configuration.

In order to have access to all commands, you must enter PRIV EXEC mode, which is the second level of access for the EXEC mode. In PRIV EXEC mode, you can enter any EXEC command, as the PRIV EXEC mode is a superset of the USER EXEC mode commands.

Most EXEC mode commands are one-time commands, such as show commands, which show the current configuration status, and clear commands, which clear counters or interfaces. EXEC mode commands are not saved across reboots of the switch.

From PRIV EXEC mode, you can enter GLOBAL CONFIG mode. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across switch reboots.

From global configuration mode you can enter a variety of protocol-specific or feature-specific configuration modes. The CLI hierarchy requires that you enter these specific configuration modes only through global configuration mode.

From global configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode.

The *Table 1.1* below summarizes all the commands available to configure and monitor WS5100 Series Switch.

Table 1.1 CLI Context Hierarchy for WS5100 Series Switch

User Exec Mode	**Priv Exec Mode**	**Global Configuration Mode**
autoinstall	acknowledge	aaa
clear	archive	access-list
clrscr	autoinstall	banner
cluster-cli	cd	boot
debug	clear	clrscr
disable	clock	country-code
enable	clrscr	crypto
exit	cluster-cli	do
help	configure	end
logout	copy	exit
no	debug	fallback
page	delete	ftp
quit	diff	help
service	dir	hostname
show	disable	interface
terminal	edit	ip
	enable	license
	erase	line
	exit	local
	halt	logging
	help	mac
	kill	no
	logout	ntp

Table 1.1 CLI Context Hierarchy for WS5100 Series Switch

User Exec Mode	Priv Exec Mode	Global Configuration Mode
	mkdir	prompt
	more	radius-server
	no	redundancy
	page	service
	ping	show
	pwd	snmp-server
	quit	terminal
	reload	timezone
	rename	username
	rmdir	wireless
	service	
	show	
	telnet	
	terminal	
	traceroute	
	upgrade	
	upgrade-abort	
	write	

1.2 Getting Context Sensitive Help

Entering a question mark (**?**) at the system prompt displays a list of commands available for each command mode. You also can get a list of the arguments and keywords available for any command with the context-sensitive help feature.

To get help specific to a command mode, a command name, a keyword, or an argument, use any of the following commands:

Command	Description
(prompt)# **help**	Displays a brief description of the help system.
*(prompt)# abbreviated-command-entry***?**	Lists commands in the current mode that begin with a particular character string.
*(prompt)# abbreviated-command-entry***<Tab>**	Completes a partial command name.
(prompt)# **?**	Lists all commands available in the command mode.
prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command.
(prompt)# command keyword ?	Lists the next available syntax option for the command.

NOTE The system prompt will vary depending on which configuration mode you are in.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called **word help**, because it completes a word for you.

```
WS5100#service?
  service  Service Commands

WS5100#service
```

To list keywords or arguments, enter a question mark (?) in place of a keyword or argument. Include a space before the **?**. This form of help is called **command syntax help**, because it shows you which keywords or arguments are available based on the command, keywords, and arguments you already have entered.

```
WS5100#service ?
  ap           access-port serviceability parameters
  clear        Reset functions
  copy         Copy from one file to another
  diag         Diagnostics
  diag-shell   Provide diag shell access
  radius       Enable radius server
```

```
  save-cli     Save CLI tree for all modes in html format
  show         Show running system information
  start-shell  Provide shell access
  tethereal    Dump and analyze network traffic
  wireless     Wireless parameters

WS5100#service
```

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the configure terminal command to config t. Because the abbreviated form of the command is unique, the switch will accept the abbreviated form and execute the command.

Entering the help command (available in any command mode) will provide the following description of the help system:

```
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100#
```

1.3 Using the no and default Forms of Commands

Almost every configuration command has a no form. In general, use the no form to disable a feature or function. Use the command without the no keyword to re enable a disabled feature or to enable a feature that is disabled by default.

1.4 Using History Command

The Symbol CCB CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries. To use the command history feature, perform any of the tasks described in the following sections:

- *Setting the History Command Buffer Size*
- *Recalling Commands*
- *Disabling the History Command Feature*

1.4.1 Setting the History Command Buffer Size

By default, the system records 256 command lines in its history buffer. To set the number of command lines that the system will record during the current terminal session, use the following command in EXEC mode:

Command	Description
WS5100# history [size number-of-lines]	Sets the size of command history buffer
WLAN Module# history	Enables command history feature

Use no history command disables the command history feature.

1.4.2 Recalling Commands

To recall commands from the history buffer, use one of the following commands or key combinations:

Command	Description
Ctrl-P or the **Up Arrow** key.	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the **Down Arrow** key.	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.
!!	Executes the last command from the command history buffer.
!<n>	Executes nth command from command history buffer.

Command	Description
`WS5100 > show history`	While in EXEC mode, lists the last several commands entered.

1.4.3 Disabling the History Command Feature

The command history feature is automatically enabled. To disable it during the current terminal session, use the following command in EXEC mode:

Command	Description
`WLAN Module# no history`	Disables command history for the current session.

1.4.4 Basic Conventions

Following are a few conventions to keep in mind while working within the command line interface:

- Always use **?** at the end of the command to view if there are any further sub modes that can be used. If yes, type the first few alphabets of the submode and press the tab key to add the submode. Continue using the **?** until you reach the final sub-submode that you would like to use for configuration of the WS5100 Series Switch.
- Pre-defined CLI commands and keywords are case-insensitive: `cfg = Cfg = CFG`. However, mostly for clarity, CLI commands and keywords are displayed in this guide using mixed case. For example, `apPolicy`, `trapHosts`, `channelInfo`.
- You can enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive.
- If an instance name (or other parameter) contains whitespace, the name must be enclosed in quotes:

```
WS5000.(Cfg)> spol "Default Switch Policy"
WS5000.(Cfg).SPolicy.[Default Switch Policy]>
```

NOTE CLI commands starting with `#`, at the `WS5100#` prompt, is ignored and is not executed.
Any leading space before a CLI command is ignored in execution

1.5 Using CLI Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the Symbol CCB CLI. The following subsections describe these features:

- *Moving the Cursor on the Command Line*
- *Completing a Partial Command Name*
- *Deleting Entries*
- *Re-displaying the Current Command Line*
- *Transposing Mistyped Characters*
- *Controlling Capitalization*

1.5.1 Moving the Cursor on the Command Line

Table 1.2 shows the key combinations or sequences you can use to move the cursor around on the command line to make corrections or changes. **Ctrl** indicates the Control key, which must be pressed simultaneously with its associated letter key. **Esc** indicates the Escape key, which must be pressed first, followed by its associated letter key. Keys are not case sensitive. Many letters used for CLI navigation and editing were chosen to provide an easy way of remembering their functions. In *Table 1.2* characters in bold inside the "***Function Summary***" column indicate the relation between the letter used and the function.

Table 1.2 Key Combinations Used to Move the Cursor

Keystrokes	Function Summary	Function Details
Left Arrow or **Ctrl-B**	Back character	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys repeatedly to scroll back toward the system prompt and verify the beginning of the command entry, or you can press the Ctrl-A key combination.
Right Arrow or Ctrl-F	Forward character	Moves the cursor one character to the right.
Esc, B	Back word	Moves the cursor back one word.
Esc, F	Forward word	Moves the cursor forward one word.
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.

Keystrokes	Function Summary	Function Details
Ctrl-E	End of line	Moves the cursor to the end of the command line.
Ctrl-d		Delete current characte
Ctrl-U		Delete text up to cursor
Ctrl-K		Delete from cursor to end of line
Ctrl-P		Get prior command from history
Ctrl-N		Get next command from history
Esc-C		Convert rest of word to uppercase
Esc-L		Convert rest of word to lowercase
Esc-D		Delete remainder of word
Ctrl-W		Delete word up to cursor
Ctrl-Z		Enter command and return to root promp
Ctrl-L		Refresh input line

1.5.2 Completing a Partial Command Name

If you cannot remember a complete command name, or if you want to reduce the amount of typing you have to perform, enter the first few letters of the command, then press the **Tab** key. The command line parser will complete the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-I instead.

The CLI will recognize a command once you have entered enough characters to make the command unique. For example, if you enter conf in privileged EXEC mode, the CLI will be able to associate your entry with the configure command, because only the configure command begins with `conf`.

In the following example the CLI recognizes the unique string for privileged EXEC mode of conf when the Tab key is pressed:

```
WLAN Module# conf<Tab>
WLAN Module# configure
```

When you use the command completion feature the CLI displays the full command name. The command is not executed until you use the **Return** or **Enter** key. This way you can modify the command if the full command was not what you intended by the abbreviation. If you enter a set of

characters that could indicate more than one command, the system lists all commands that begin with that set of characters.

Alternatively, enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter you enter and the question mark (?).

For example, entering `co?` will list all commands available in the current command mode:

```
WLAN Module# co?
copy? commit
WLAN Module# co
```

NOTE The characters you enter before the question mark are reprinted to the screen to allow you to complete the command entry.

1.5.3 Deleting Entries

Use any of the following keys or key combinations to delete command entries if you make a mistake or change your mind:

Keystrokes	Purpose
Backspace	Deletes the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-W	Deletes the word up to the cursor.
Esc, D	Deletes from the cursor to the end of the word.

1.5.4 Re-displaying the Current Command Line

If you are entering a command and the system suddenly sends a message to your screen, you can easily recall your current command line entry. To redisplay the current command line (refresh the screen), use either of the following key combinations:

Keystrokes	Purpose
Ctrl-L	Redisplays the current command line.

1.5.5 Command Output pagination

When working with the Symbol CCB CLI, output often extends beyond the visible screen length. For cases where output continues beyond the bottom of the screen, such as with the output of many **?** or show commands, the output is paused and `Press Any Key to Continue (Q to Quit)` prompt is displayed at the bottom of the screen. To resume output, press the Return key to scroll down one line, or press the Spacebar to display the next full screen of output.

1.5.6 Transposing Mistyped Characters

If you have mistyped a command entry, you can transpose the mistyped characters. To transpose characters, use the following key combination:

Keystrokes	Purpose
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.

1.5.7 Controlling Capitalization

You can capitalize or lowercase words or capitalize a set of letters with simple key sequences. Note, however, that Symbol CCB commands are generally case-insensitive, and are typically all in lowercase. To change the capitalization of commands, use any of the following key sequences:

Keystrokes	Purpose
Esc, C	Capitalizes the letters at the right of cursor.
Esc, L	Changes the letters at the right of cursor to lowercase.

2

Common Commands

This chapter explains the common CLI commands used amongst the USER EXEC and PRIV EXEC modes.

PRIV EXEC command set contains all of the commands available in USER EXEC mode, some commands can be entered in either mode. Commands that can be entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If user or privileged is not specified in the documentation, assume that you can enter the referenced commands in either mode.

2.1 Common Commands

Table 2.1 summarizes the commands common amongst many contexts and instance contexts within the WS5100 Series Switch command line interface.

Table 2.1 Common commands amongst most contexts

Command	Description	Ref.
clrscr	Clears the display screen.	page 2-3
exit	End current mode and down to previous mode.	page 2-4
help	Description of the interactive help system.	page 2-5
no	Negate a command or set its defaults.	page 2-7
service	Service Commands.	page 2-8
show	Shows running system information.	page 2-20
terminal	Set terminal line parameters.	page 2-19

2.1.1 clrscr

Common Commands

Use this command to clear the screen displaying the cli and start afresh at the prompt (**#**).

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#clrscr
```

2.1.2 exit

Common Commands

Use this command to end current mode and move to the previous mode.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config)#exit
```

2.1.3 help

Common Commands

Use this command to get access to the advanced help feature. You can also use "**?**" anytime at the command prompt to get access to the help topic.

When using this command, if nothing matches then the help list will be empty and you must backup until entering a '**?**' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show ve?'.)

Syntax

```
help
```

or

```
?
```

Parameters

None.

Usage Guidelines

Example

```
WS5100>show ?
  autoinstall         autoinstall configuration
  banner              Display Message of the Day Login banner
  commands            Show command lists
  crypto              crypto
  environment         show environmental information
  history             Display the session command history
  interfaces          Interface status and configuration
  ip                  Internet Protocol (IP)
  ldap                ldap server
  licenses            Show any installed licenses
  logging             Show logging configuration and buffer
  mac                 Media Access Control
  management          Display L3 Managment Interface name
  mobility            Display Mobility Parameters
```

```
  ntp                 Network time protocol
  privilege           Show current privilege level
  radius              Radius configuration commands
  redundancy-group    Display redundancy group parameters
  redundancy-history  Display state transition history of the switch.
  redundancy-members  Display redundancy group members in detail
  snmp                Display SNMP engine parameters
  snmp-server         Display SNMP engine parameters
  terminal            Display terminal configuration parameters
  timezone            Display timezone
  users               Display information about terminal lines
  version             Display software & hardware version
  wireless            Wireless configuration commandsE

WS5100>show autoinstall ?
  |  Output modifiers
  >  Output redirection
  >>  Output redirection appending
```

2.1.4 no

Common Commands

Use this command to either negate a command or set its defaults.

Syntax

no

Parameters

None.

Usage Guidelines

Example

```
WS5100>no ?
  autoinstall  autoinstall configuration command
  cluster-cli  Cluster context
  debug        Debugging functions
  page         Toggle paging
  service      Service Commands
```

2.1.5 service

Common Commands

Use this command to servie/debug the WS5100 Series Switch.

Syntax

```
service (diag (enable | led ( 1 (amber ( flashing|off|on) | blue | red ) |
2 (amber ( flashing|off|on) | blue | red ) ) | limit
(buffer|fan|filesys(etc2|flash|ram)|load(1|15|5)|maxFDs|pkbuffers|procRAM|
ram|routecache|tempreature) |period <100-30000>)|save-cli|show (cli|
command-history|crash-info|diag|info|memory|natstats|process|
reboot-history|rulestats|startup-log|upgrade-history))
```

Parameters

diag	Diagnostics
save-cli	Save CLI tree for all modes in html format.
show	Show running system information
enable	Enables the service diagnostics mode
led	Use to configure LED display sequence
1	Use to configure upper LED. You can select from the following options: • amber • blue • red
2	Use to configure lower LED.You can select from the following options • amber • blue • red
limit	Use to set the diagnostic limit submodes/commands.

buffer	Use to configure the buffer usage warning limit. The warning limit can be set to one of the following buffer limit size: • 12 – 128 byte buffer limit • 128k – 128k byte buffer limit • 16k –- 16k byte buffer limit • 1k – 1k byte buffer limit • 256 – 256 byte buffer limit • 2k – 2k byte buffer limit • 32 – 32 byte buffer limit • 32k – 32k byte buffer limit • 4k – 4k byte buffer limit • 512 – 512 byte buffer limit • 64 – 64 byte buffer limit • 64k – 64k byte buffer limit • 8k – 8 byte buffer limit
fan	Use to set the fan speed limit. You can configure the fan speed limit for both, Fan 1 and Fan 2.
filesys	Use to set file system freespace limit. You can select the freespace limit for the following sub context: • etc2 • flash • ram
load	Use to configure aggregate processor load. You can select from the following submodes: • 1 – Aggregate processor load during the previous minute. • 15 – Aggregate processor load during the previous 15 minute. • 5 – Aggregate processor load during the previous 5 minute.
maxFDs	Use to configure the maximum number of file descriptors. You can set anything between 0 to 32767 file descriptors.

pkbuffers	Use to configure and set the packet buffer head cache limit. You can set anything between 0 to 65535 as the buffer cache limit.
procRAM	Use to configure the RAM space used by a process. You can set he percentage of RAM space to be used by the processor from anything between 0.0 ti 100.0 percent.
ram	Use to configure the free space for the RAM. You can configure the free space to anything between 0.0 to 100.0 percent.
routecache	Use to configure the IP route cache usage. Can be set with an value between 0 - 65553
temperature	Use to set the temperature sensor for the WS5100 Series Switch. You can set as many as 8 temperature sensors.
period	Use to set diagnostic period
<100-30000>	Use to configure Diagnostics period. You can set a value of anything between 100-30000 milli seconds. The default value is set to 1000 milliseconds.
save-cli	This command creates clitree.html which saves and displays the cli tree for all modes.
cli	Show CLI tree of current mode
command-history	Display command (except show commands) history
crash-info	Display information about core, panic and AP dump files
diag	Diagnostics
info	Show snapshot of available support information
memory	Show memory statistics
natstats	Show ACL rule stats
process	Show processes (sorted by memory usage)
reboot-history	Show reboot history
rulestats	Show ACL rule stats
startup-log	Show startup log

upgrade-history	Show upgrade history

Usage Guidelines

Example

```
WS5100#service diag ?
  enable  Enable in service diagnostics
  led     LED control
  limit   diagnostic limit command
  period  Set diagnostics period

WS5100#service diag enable

WS5100#service diag led ?
  1  1 - upper LED
  2  2 - lower LED

WS5100#service diag led 1 ?
  amber  amber
  blue   blue
  red    red

WS5100#service diag led 1 amber ?
  flashing  LED Flashing
  off       LED off
  on        LED on

WS5100#service diag led 1 amber flashing
WS5100#service diag led 1 amber flashing
WS5100#service diag led 1 blue on
WS5100#service diag led 1 red off
WS5100#service diag led 2 amber flashing

WS5100#service diag limit ?
  buffer       buffer usage warning limit
  fan          Fan speed limit
  filesys      file system freespace limit
  load         agregate processor load
  maxFDs       maximum number of file descriptors
  pkbuffers    packet buffer head cache
  procRAM      percent RAM used by a process
  ram          percent free RAM
  routecache   IP route cache usage
  temperature  temperature limit
WS5100#service diag limit buffer ?
  128   128 byte buffer limit
```

```
  128k  128k byte buffer limit
  16k   16k byte buffer limit
  1k    1k byte buffer limit
  256   256 byte buffer limit
  2k    2k byte buffer limit
  32    32 byte buffer limit
  32k   32k byte buffer limit
  4k    4k byte buffer limit
  512   512 byte buffer limit
  64    64 byte buffer limit
  64k   64k byte buffer limit
  8k    8k byte buffer limit

WS5100#service diag limit buffer 32k ?
  <0-65535>  buffer usage warning limit 0-65535

WS5100#service diag limit buffer 32k 4096

WS5100#service diag limit fan ?
  <1-2>  Fan number

WS5100#service diag limit fan 1 ?
  low  Low speed limit

WS5100#service diag limit fan 1 low ?
  <1000-15000>  Limit value from 1000 to 15,000

WS5100#service diag limit fan 1 low 1100
WS5100#service diag limit fan 2 low 10000
WS5100#Sep 01 15:51:54 2006: %DIAG-4-FANUNDERSPEED: Fan case under speed:
8881 RPM is under limit 10000 RPM

WS5100#service diag limit filesys ?
  etc2   /etc2 file system
  flash  /flash file system
  ram    /ram file system

WS5100#service diag limit filesys flash ?
  WORD  limit from 0.0 to 100.0

WS5100#service diag limit filesys flash 20
WS5100#service diag limit filesys etc2 10
WS5100#service diag limit filesys ram 30



WS5100#service diag limit load ?
  1   during the previous minute
  15  during the previous 15 minutes
```

```
  5   during the previous five minutes

WS5100#service diag limit load 5 ?
  WORD  percentage load from 0.0 to 100.0

WS5100#service diag limit load 5 50

WS5100#service diag limit maxFDs ?
  <0-32767>  0-32767

WS5100#service diag limit maxFDs 30000

WS5100#service diag limit pkbuffers ?
  <0-65535>  limit from 0-65535

WS5100#service diag limit pkbuffers 4096
WS5100#service diag limit procRAM ?
  WORD  limit from 0.0-100.0

WS5100#service diag limit procRAM 10

WS5100#service diag limit ram ?
  WORD  limit from 0.0-100.0

WS5100#service diag limit ram 20

WS5100#service diag limit routecache ?
  <0-65535>  limit from 0-65535

WS5100#service diag limit routecache 10240

WS5100#service diag limit temperature ?
  <1-8>  temperature sensor number

WS5100#service diag period ?
  <100-30000>  Diagnostics period <100-30000> default 1000 milliseconds

WS5100#service diag period 20000

WS5100#service save-cli

/usr/scripts/genclitree.sh: /usr/scripts/genclitree.sh: 15: eth: not found
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
WS5100#



WS5100>service show cli
```

```
User Exec mode:
+-autoinstall
  +-cluster-config
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-config
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-image
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-start [autoinstall start]
+-clear
  +-crypto
    +-ike
      +-sa [clear crypto ike sa ( A.B.C.D |)]
        +-A.B.C.D [clear crypto ike sa ( A.B.C.D |)]
    +-ipsec
      +-sa [clear crypto ipsec sa (A.B.C.D |)].....
```

WS5100>service show command-history

```
Configured size of command history is 200

  Date & Time          User  Location   Command
======================================================================
Aug 31 23:40:15 2006   (null)     vty 131     wireless
Aug 31 23:40:15 2006   (null)     vty 131     config t
Aug 31 23:40:15 2006   (null)     vty 131     enable
Aug 31 23:40:14 2006   (null)     vty 131     interface eth0
Aug 31 23:40:14 2006   (null)     vty 131     config t
Aug 31 23:40:14 2006   (null)     vty 131     enable
Aug 31 23:40:13 2006   (null)     vty 131     line console 0
Aug 31 23:40:13 2006   (null)     vty 131     config t
Aug 31 23:40:13 2006   (null)     vty 131     enable
Aug 31 23:40:12 2006   (null)     vty 131     config t
Aug 31 23:40:12 2006   (null)     vty 131     enable
Aug 31 23:40:11 2006   (null)     vty 131     enable
Aug 31 16:30:14 2006   (null)     con 0     configure terminal
Aug 31 16:30:04 2006   (null)     con 0     en
Aug 31 16:29:21 2006   (null)     con 0     exit
Aug 30 19:54:13 2006   (null)     vty 130     enable
Aug 30 19:53:09 2006   (null)     vty 130     disable
Aug 30 19:41:12 2006   (null)     vty 130     clear mobility peer-
statistics 157.235.208.39
```

WS5100>service show crash-info

```
Coredump files:
Name                     Size    Date & Time
=============================================
imish_8990_200B.core.gz 299.5k   Aug 31 23:50

WS5100>
```

WS5100>service show info

```
4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.1M out of 18.6M available for crashinfo.

List of Files:

imish_8990_200B.core.gz         299.5k  Aug 31 23:50
messages.log                    200     Aug 30 15:32
snmpd.log                       316     Aug 30 15:33
startup.log                     16.5k   Aug 30 15:32
command.history                 9.6k    Aug 31 23:40
reboot.history                  2.3k    Aug 30 15:32
upgrade.history                 782     Aug 29 18:32

Please export these files or delete them for more space.

WS5100>
```

WS5100>service show memory

```
MemTotal:       256220 kB
MemFree:        155628 kB
Buffers:          1596 kB
Cached:          27912 kB
SwapCached:          0 kB
Active:          53832 kB
Inactive:        16272 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       256220 kB
LowFree:        155628 kB
SwapTotal:           0 kB
SwapFree:            0 kB
Dirty:               0 kB
Writeback:           0 kB
Mapped:          50768 kB
Slab:             9984 kB
CommitLimit:    128108 kB
Committed_AS:    75368 kB
PageTables:        468 kB
```

```
VmallocTotal:   778200 kB
VmallocUsed:     19568 kB
VmallocChunk:   757824 kB
WS5100>

WS5100>service show process
  PID  STATUS   RSS  PPID %CPU %MEM COMMAND
  320  S        10M     1  0.0  4.1 ccsrvr
  345  S       8488     1  1.9  3.3 ccstatsd
  387  S       5612     1  0.0  2.1 securitymgr
  318  S       4480     1  0.0  1.7 snmpd
  394  S       3932     1  0.0  1.5 imi
  349  R       3424     1  0.0  1.3 isDiag
  367  S       3264   279  0.0  1.2 radconfd
  315  S       3208   279  0.0  1.2 CertMgr
  391  S       3104     1  0.0  1.2 radiusd
  373  S       2844     1  0.0  1.1 dhcpsvr
  319  S       2744     1  0.0  1.0 licenseMgr
 6823  S       2712   429  0.0  1.0 imish
 6770  S       2668     1  0.0  1.0 imish
  363  S       1824     1  0.0  0.7 nsm
  339  S       1736   279  0.0  0.6 fileMgmt
  291  S       1676     1  0.0  0.6 logd
  375  S       1672     1  0.0  0.6 wccpd
  279  S       1636     1  0.0  0.6 pmd
  430  S       1636     1  0.0  0.6 stunnel
 1370  S       1512     1  0.0  0.5 sshd
  346  S       1448     1  0.0  0.5 mobd
  340  S       1308   279  0.0  0.5 fileXferd.................

WS5100> service show reboot-history
Configured size of reboot history is 50

  Date & Time             Event
=====================================================
Aug 30 15:32:39 2006     startup
Aug 30 15:31:17 2006     shutdown (graceful:user)
Aug 30 13:31:13 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 29 18:40:38 2006     startup
Aug 29 18:39:15 2006     shutdown (graceful:user)
Aug 28 12:38:09 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 23 13:33:02 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 21 13:10:09 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 17 15:10:21 2006     startup
Aug 17 15:08:58 2006     shutdown (graceful:user)
```

```
Aug 16 13:48:41 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 11 19:32:55 2006     startup
Aug 11 19:31:32 2006     shutdown (graceful:user)
```

WS5100> service show startup-log

```
Aug 30 15:32:43 2006: %KERN-5-NOTICE: Linux version 2.6.13.4-ws-symbol
(wios-eng@wios-build) (gcc version 3.4.5) #1.
Aug 30 15:32:43 2006: %KERN-6-INFO: BIOS-provided physical RAM map:.
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 0000000000000000 -
000000000009fc00 (usable).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 000000000009fc00 -
00000000000a0000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000000e0000 -
0000000000100000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 0000000000100000 -
000000000ff40000 (usable).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 000000000ff40000 -
000000000ff50000 (ACPI data).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 000000000ff50000 -
0000000010000000 (ACPI NVS).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000fec80000 -
00000000fec81000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000fff80000 -
0000000100000000 (reserved).
Aug 30 15:32:43 2006: %KERN-5-NOTICE: 255MB LOWMEM available..
Aug 30 15:32:43 2006: KERN: On node 0 totalpages: 65344.
Aug 30 15:32:43 2006: KERN:   DMA zone: 4096 pages, LIFO batch:1.
Aug 30 15:32:43 2006: KERN:   Normal zone: 61248 pages, LIFO batch:31.
Aug 30 15:32:43 2006: KERN:   HighMem zone: 0 pages, LIFO batch:1.
Aug 30 15:32:43 2006: %KERN-6-INFO: DMI 2.3 present..
Aug 30 15:32:43 2006: KERN: ACPI: RSDP (v000 ACPIAM
) @ 0x000f7720.
Aug 30 15:32:43 2006: KERN: ACPI: RSDT (v001 A M I  OEMRSDT  0x09000512
MSFT 0x00000097) @ 0x0ff40000.
Aug 30 15:32:43 2006: KERN: ACPI: FADT (v002 A M I  OEMFACP  0x09000512
MSFT 0x00000097) @ 0x0ff40200.
Aug 30 15:32:43 2006: KERN: ACPI: MADT (v001 A M I  OEMAPIC  0x09000512
MSFT 0x00000097) @ 0x0ff40300.
Aug 30 15:32:43 2006: KERN: ACPI: OEMB (v001 A M I  OEMBIOS  0x09000512
MSFT 0x00000097) @ 0x0ff50040.
Aug 30 15:32:43 2006: KERN: ACPI: DSDT (v001  1ABVF 1ABVF007 0x00000007
INTL 0x02002026) @ 0x00000000.
```

WS5100> service show upgrade-history

```
Configured size of upgrade history is 50

  Date & Time            Old Version     New Version     Status
=====================================================================
Aug 29 18:30:43 2006 3.0.0.0-180B 3.0.0.0-200B Successful
Aug 17 15:07:03 2006 3.0.0.0-17872X 3.0.0.0-180B Successful
Aug 11 19:29:41 2006 3.0.0.0-170B 3.0.0.0-17872X Successful
Aug 11 19:28:52 2006 3.0.0.0-170B 3.0.0.0-170B Unable to get update file.
tftp: server says: File not found
Aug 09 17:30:25 2006 3.0.0.0-17174X 3.0.0.0-170B Successful
Jul 26 15:17:14 2006 3.0.0.0-140D 3.0.0.0-17174X Successful
Jul 26 15:16:40 2006 3.0.0.0-140D 3.0.0.0-140D Unable to get update file.
tftp: server says: File not found
Jul 26 15:16:08 2006 3.0.0.0-140D 3.0.0.0-140D Unable to get update file.
tftp: C: Unknown host
Jul 19 19:52:38 2006 3.0.0.0-16786X 3.0.0.0-140D Successful
Jul 19 19:52:07 2006 3.0.0.0-16786X 3.0.0.0-16786X Unable to get update
file. tftp: server says: File not found
WS5100>
```

2.1.6 terminal

Common Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(length <0-512>|no(length <0-512>|width)|width <0-512> )
```

Parameters

length	Set number of lines on a screen.
no	Negate a command or set its defaults.
width	Sets width/ number of characters on a screen line.

Usage Guidelines

Example

```
WS5100>terminal length 100
WS5100>

WS5100>terminal width 200
WS5100>
```

2.2 show

▶ *Common Commands*

This command is used to display the settings for the specified system component. There are a number of ways to invoke the show command:

- Invoked without any arguments, show displays information about the current context. If the current context contains instances, then show command (usually) displays a list of these instances.
- Invoked with the display_parameter, it displays information about that component.

Syntax

```
show [display_parameter]
```

Parameters

Display Parameters	Description	Mode	Example
autoinstall	Displays autoinstall configuration.	Common	page 2-22
banner	Displays message of the day login banner.	Common	page 2-23
commands	Displays command lists.	Common	page 2-24
crypto		Common	page 2-25
environment	Displays environmental information.	Common	page 2-29
history	Displays the session command history.	Common	page 2-29
interfaces	Displays interface status and configuration.	Common	page 2-30
ip	Displays internet protocol.	Common	page 2-32
ldap	Displays ldap server configuration parameters.	Common	page 2-38
licenses	Displays the installed licenses, if any.	Common	page 2-40
logging	Displays logging configuration and buffer.	Common	page 2-41
mac	Displays media access control IP configuration.	Common	page 2-42
management	Displays L3 management interface name.	Common	page 2-43
mobility	Displays mobility parameters.	Common	page 2-44

Display Parameters	Description	Mode	Example
ntp	Displays network time protocol.	Common	page 2-47
privilege	Displays current privilege level.	Common	page 2-49
radius	Displays radius configuration commands.	Common	page 2-50
redundancy-group	Displays redundancy group parameters.	Common	page 2-51
redundancy-history	Displays state transition history of the switch.	Common	page 2-53
redundancy-members	Displays redundancy group members in detail.	Common	page 2-54
snmp	Displays SNMP engine parameters.	Common	page 2-55
snmp-server	Displays SNMP engine parameters.	Common	page 2-56
terminal	Displays terminal configuration parameters.	Common	page 2-59
timezone	Displays timezone.	Common	page 2-60
users	Displays information about terminal lines.	Common	page 2-61
version	Displays software and hardware version.	Common	page 2-62
wireless	Displays wireless configuration commands.	Common	page 2-63
access-list	Displays access list Internet Protocol (IP) configuration.	Privilege/ Global Config	page 2-70
alarm-log	Displays all alarms currently in the system.	Privilege/ Global Config	page 2-71
boot	Displays boot configuration.	Privilege/ Global Config	page 2-72
clock	Displays system clock.	Privilege/ Global Config	page 2-73
debugging	Displays debugging setting.	Privilege/ Global Config	page 2-74
file	Displays filesystem information.	Privilege/ Global Config	page 2-75

Display Parameters	Description	Mode	Example
ftp	Displays FTP Server configuration.	Privilege/ Global Config	page 2-76
password-encryption	Displays password encryption.	Privilege/ Global Config	page 2-77
running-config	Displays current operating configuration.	Privilege/ Global Config	page 2-78
securitymgr	Displays debug info for ACL, VPN and NAT.	Privilege/ Global Config	page 2-81
sessions	Displays current active open connections.	Privilege/ Global Config	page 2-82
startup-config	Displays contents of startup configuration.	Privilege/ Global Config	page 2-83
upgrade-status	Displays last image upgrade status.	Privilege/ Global Config	page 2-84

2.2.1 autoinstall

▶ *Common to all modes*

Syntax

```
show autoinstall
```

Parameters

None.

Example

```
WS5100>show autoinstall
WS5100>
```

2.2.2 banner

Common to all modes

Syntax

```
show banner
```

Parameters

motd	Use this to enter *Message of the Day* banner

Example

```
WS5100>show banner motd
Welcome to CLI
WS5100>
```

2.2.3 commands

Common to all modes

Syntax

```
WS5100>show commands
```

Parameters

None.

Example

```
WS5100>show commands
  autoinstall (config|cluster-config|image) enable
  autoinstall (config|cluster-config|image) url LINE
  autoinstall (config|cluster-config|image) enable
  autoinstall (config|cluster-config|image) url LINE
  autoinstall (config|cluster-config|image) enable
  autoinstall (config|cluster-config|image) url LINE
  autoinstall start
  clear crypto ike sa ( A.B.C.D |)
  clear crypto ike sa ( A.B.C.D |)
  clear crypto ipsec sa (A.B.C.D |)
  clear crypto ipsec sa (A.B.C.D |)
  clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
  clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
  clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
  clear mobility mu (AA-BB-CC-DD-EE-FF|home-database|foreign-database|all)
  clear mobility mu-log
  clear mobility peer-log
  clear mobility peer-statistics (A.B.C.D|)
  clear mobility peer-statistics (A.B.C.D|)
  clear wireless-statistics
  clrscr
  cluster-cli enable
  debug certmgr ( error|info|all )
  debug certmgr ( error|info|all )
  debug certmgr ( error|info|all )
  debug ip ssh
  debug mobility (cc|error|forwarding|mu|packet|peer|system)
  debug mobility (cc|error|forwarding|mu|packet|peer|system)
  debug mobility (cc|error|forwarding|mu|packet|peer|system)
  debug mobility (cc|error|forwarding|mu|packet|peer|system)
  debug mobility (cc|error|forwarding|mu|packet|peer|system)
  debug mobility (cc|error|forwarding|mu|packet|peer|system)
  debug mobility (cc|error|forwarding|mu|packet|peer|system)
-- MORE --, next page: Space, next line: Enter, quit: Control-C
.................................................(contd)
```

2.2.4 crypto

▶ *Common to all modes*

Syntax

```
show crypto(ipsec|isakmp|key|map|pki)

show crypto ipsec(sa|security-association(lifetime)|transformset)
show crypto isakmp(policy(<1-10000>)|sa)
show crypto key(mypubkey)
show crypto map(interface|tag)
show crypto pki(request|trustpoints)
```

Parameters

ipsec	ipsec
sa	security association
security-association	security association
lifetime	lifetime
transformset	transformset
isakmp	isakmp
policy	policy
sa	security association
key	Authentication key management
mypubkey	Public Key
map	map
interface	interface
tag	tag
pki	Public Key Infrastructure commands
request	Certificate Request
trustpoints	Show trustpoints

Usage Guidelines

Security engine periodically updates the IPSec and Isakamp statistics for every 60 seconds.

Example

```
WS5100(config)#show crypto pki request tptest
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUQCAQAwaDELMAkGA1UEBhMCaW4xEjAQBgNVBAgTCWthcm5hdGFrYTES
MBAGA1UEBxMJYmFuZ2Fsb3JlMQ8wDQYDVQQKEwZzeW1ib2wxDDAKBgNVBAsTA3dp
ZDESMBAGA1UEAxMJdGVzdC1jZXJ0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC3qisZdTn7rKzv5TrGtKt7fwMwaYpgehyl52I4fDLZYY/WTTTJFyKwW6s+Pq2R
mM9oiqX8mCZeSEIJIATpAVT2M5Ukb4Br9YQDcWHs84oXRJxKPeZ3WscBld2soPvK
ui1LoizZH9iqawmkXED1TFMBbDWiOcfnqQKn8Tddeax/JQIDAQABoDMwMQYJKoZI
hvcNAQkOMSQwIjALBgNVHQ8EBAMCBLAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJ
KoZIhvcNAQEEBQADgYEAoJMylm3aaY1CnkOO5TbxB+qL4F4MKL6+o/m0yRPqy/2S
gkk/OwxHvc3TbA9WjbKkFWIDyqU7X0d+c8f9KogwxDwWHll2IBiTCtBAq6hpgKOv
Um9GFvMFps9XVkKtYttN3fer9tA+6xY9CKlr12mNGOYFHyVjMc3Pic0ODFiPHAU=
-----END CERTIFICATE REQUEST-----

WS5100(config)#show crypto pki trustpoints

Trustpoint :default-trustpoint
------------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:         Symbol Technologies
    Issuer Name:
      Common Name:         Symbol Technologies
  Valid From:   Sep 13 16:14:49 2006 GMT
  Valid Until:  Sep 13 16:14:49 2007 GMT

Trustpoint :tptest
------------------------------------------------
  CA certificate configured
    Subject Name:
      Common Name:         monarch
      Organizational Unit: wid
      Organization:        symbol
      Location:            bangalore
      State:               karnataka
      Country:             in
      email:               testuser@domain.com
    Issuer Name:
      Common Name:         monarch
      Organizational Unit: wid
      Organization:        symbol
      Location:            bangalore
      State:               karnataka
      Country:             in
```

```
    email:               testuser@domain.com
Valid From:   Sep 11 05:48:52 2006 GMT
Valid Until:  Sep 11 05:48:52 2007 GMT
```

2.2.5 environment

Common to all modes

Syntax

```
show environment
```

Parameters

None.

Example

```
WS5100>show environment
       CPU temperature :  33.0 C
       system temperature :  33.0 C
       CPU fan         :  4354 rpm
       case fan         :  8766 rpm
WS5100>
```

2.2.6 history

▶ *Common to all modes*

Syntax

```
show history
```

Parameters

None.

Example

```
WS5100>show history
   1 show
   2 clrscr
   3 enable
   4 clrscr
   5 configure terminal
   6 exit
   7 clrscr
   8 show history
WS5100>
```

2.2.7 interfaces

Common to all modes

Syntax

```
show interfaces(IFNAME|eth <1-2>|switchport|tunnel|vlan)
```

Parameters

IFNAME	
eth	
switchport	
tunnel	
vlan	

Usage Guidelines

Example

```
WS5100(config)#show interfaces eth1
Interface eth1
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-a0-f8-65-
b0-4e
  index 2 metric 1 mtu 1500  <UP,BROADCAST,RUNNING,MULTICAST>
  Speed: Admin Auto, Operational 100M
  Duplex: Admin Auto, Operational Full
  Switchport Settings: Mode: Access, Access Vlan: 2100
    input packets 38766, bytes 9483540, dropped 0, multicast packets 13377
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 4, bytes 336, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

WS5100(config)#show interfaces switchport eth1
Interface eth1
  Switchport Settings: Mode: Access, Access Vlan: 2100

WS5100(config)#show interfaces switchport vlan1
Interface vlan1
  Switchport Settings: Mode: Access, Access Vlan: 0
```

```
WS5100(config)#interface tunnel 1
WS5100(config-if)#Sep 14 18:38:17 2006: %DAEMON-5-NOTICE:
WIOS_SECURITYMGR[414]: DNSALG: Shutting down.
Sep 14 18:38:17 2006: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[414]: FTPALG:
Shutting down.
Sep 14 18:38:17 2006: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[414]: FTPALG:
Application gateway started.
Sep 14 18:38:17 2006: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[414]: DNSALG:
Application gateway started


WS5100(config-if)#show interfaces tunnel 1
Interface tunnel1
  Hardware Type Tunnel, Interface Mode Layer 3
  index 9 metric 1 mtu 1476  <UP,RUNNING,NOARP>
  Tunnel source UNKNOWN, destination UNKNOWN
  Tunnel protocol/transport GRE/IP,  Tunnel TTL 255
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

2.2.8 ip

Common to all modes

Syntax

```
show ip (access-group (IFNAME | eth <1-2> | vlan <1-4094>) | arp |
ddns(binding)| dhcp-vendor-options | domain-name |
http(secure-server|server)| interface(IFNAME|brief|tunnel|vlan) |
name-server | route(A.B.C.D|A.B.C.D/M|detail) | routing | ssh | telnet )

show ip access-group (IFNAME|eth <1-2> |vlan <1-4094>)
Show ip access-group <interface-name>
show ip arp
show ip ddns(binding)
show ip dhcp(binding|pool)
show ip dhcp-vendor-options
show ip domain-name
show ip http(secure-server|server)
show ip interface(IFNAME|brief|tunnel|vlan)
show ip name-server
show ip route(A.B.C.D|A.B.C.D/M|detail)
show ip routing
show ip ssh
show ip telnet
```

Parameters

access-group	Display ACLs attached to an interface
IFNAME	The name of the interface to which the ACL is associated. It lists the details of ACLs configured on the particular Layer 3 or Layer 2 interface.
eth	The name of the ethernet interface to which the ACL is associated.
vlan	The name of the VLAN interface to which the ACL is associated.
arp	Display Address Resolution Protocol
ddns	Displays DDNS configuration
binding	DNS Address bindings
dhcp	Displays DHCP Server Configuration
binding	DNS Address bindings
pool	DHCP Pools

dhcp-vendor-options	DHCP Option 43 parameters received from DHCP server
domain-name	Default domain for DNS
http	Hyper Text Transfer Protocol
secure-server	Secure HTTP server
server	HTTP server
interface	IP interface status and configuration
IFNAME	Interface name
brief	Brief summary of IP status and configuration
tunnel	Tunnel Interface
vlan	Vlan Interface
name-server	DNS nameservers
route	IP routing table
A.B.C.D	Network in the IP routing table to display
A.B.C.D/M	IP prefix <network>/<length>, e.g., 35.0.0.0/8
detail	IP routing table in detail
routing	IP routing status
ssh	Secured Shell (SSH) server
telnet	Telnet server

Usage Guidelines

1. It has been noted that the interface status and vlan status is displayed as UP inspite of a disconnection. In such a case you need to shutdown the vlan. Follow the steps gievn below:
   a. Check the status of interface and vlan using:

```
WS5100(config)#show ip interface brief
Interface            IP-Address           Status              Protocol
vlan1                 157.235.208.69(DHCP)   up                    up
vlan3                 unassigned             up                    up
WS5100(config)#
```

   b. If the stauts of the VLAN is UP even if eth1 / eth2 is diconnected then shutdown the VLAN associated with eth1 using:

```
WS5100(config-if)#show ip interface vlan 3 brief
Interface            IP-Address           Status              Protocol
vlan3                 unassigned             up                    up
WS5100(config-if)#shutdown
```

   c. Now check the stauts and you will note that VLAN has now been disassociated and the status is now DOWN.

```
WS5100(config)#show ip interface brief
Interface            IP-Address           Status              Protocol
vlan1                 157.235.208.69(DHCP)   up                    up
vlan3                unassigned            administratively down down
WS5100(config)#
```

2. The above instance may also happen when a DHCP interface is disconnected. The DHCP is not effected though because it runs on a virtual interface and not on teh physical interface. In this case it is the physical interface that is disconnected not hte virtual interface. In WS5100, when the ethernet interface comes back up, it will restart the dhcp client on any virtual interfaces (SVIs) of which the physical interface is a member port. This ensures that if the interface was disconnected and reconnected to a different interface it will get a new ip address, route, name server, domain name etc. corresponding to the new dhcp server/ scope.

Example

```
WS5100(config)#show ip access-group eth 1
Interface eth1
  Inbound IP Access List :
  Inbound MAC Access List :
WS5100(config)#show ip access-group vlan 1
Interface vlan1
  Inbound IP Access List :
WS5100(config)#show ip access-group eth2
Interface eth2
  Inbound IP Access List :
  Inbound MAC Access List :

WS5100#show ip dhcp binding
IP              MAC/Client-Id      Type       Expiry Time
--              -------------      ----       -----------

WS5100#show ip dhcp pool
!
ip dhcp pool pl
!
ip dhcp pool pool1
 domain-name test.com
 bootfile 123
 network 10.10.10.0/24
 address range 10.10.10.2 10.10.10.30
!
ip dhcp pool poo110
 next-server 1.1.1.1
 netbios-node-type b-node

WS5100#show ip dhcp-vendor-options
Server Info:
Firmware Image File:
Config File:
Cluster Config File:

WS5100#show ip domain-name
 IP domain-lookup : Enable
 Domain Name   : symbol.com

WS5100#show ip http server
HTTP server: Running
Config status: Enabled
```

```
WS5100#show ip http secure-server
HTTP secure server: Running
Config status: Enabled
Trustpoint: default-trustpoint

WS5100#show ip interface brief
Interface             IP-Address            Status                Protocol
vlan1                 157.235.208.233(DHCP)  up                    up
tunnel1               unassigned             up                    up

WS5100#show ip interface tunnel 1 ?
  brief  Brief summary of IP status and configuration

WS5100#show ip interface tunnel 1 brief
Interface             IP-Address            Status                Protocol
tunnel1               unassigned             up                    up

WS5100#show ip interface vlan 1 brief
Interface             IP-Address            Status                Protocol
vlan1                 157.235.208.233(DHCP)  up                    up

WS5100#show ip name-server
157.235.3.195           dynamic
157.235.3.196           dynamic

WS5100#show ip nat translations inside source
S/D Dir Actual Address              NATed Address          ACL
Overload-If

WS5100#show ip nat translations outside destination
S/D Dir Actual Address              NATed Address          ACL
Overload-If

WS5100#show ip routing
IP routing is on

WS5100(config)#show ip route detail
Codes: K - kernel/icmp, C - connected, S - static, D - DHCP
       > - Active route,  - Next-hop in FIB, p - stale info

S       1.1.0.0/16 [1/0] via 1.1.1.1 inactive
S       1.1.1.0/24 [1/0] via 1.1.1.2 inactive
S       10.0.0.0/8 [1/0] via 10.10.10.10 inactive
S       157.235.208.0/24 [1/0] via 157.235.208.246 inactive
```

```
WS5100#show ip ssh
SSH server: enabled
Status: running
Keypair name: default_ssh_rsa_key
Port: 22

WS5100#show ip telnet
Telnet server: enabled
Status: running
Port: 23
```

2.2.9 ldap

Common to all modes

Syntax

```
show ldap(configuration(primary|secondary))
```

Parameters

ldap	LDAP Server
configuration	ldap server configuration parameters
primary	primary ldap server
secondary	secondary ldap server

Example

```
WS5100(config-radsrv)#show ldap configuration
LDAP Server Config Details
_________________________

Primary LDAP Server configuration

        IP Address             : 10.10.10.1
        Port                   : 369
        Login                  :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
        Bind DN                :
cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                : ou=symbol,dc=activedirectory,dc=com
        Password               : 0 symbol@123
        Password Attribute     : UserPassword
        Group Name             : cn
        Group Membership Filter: (&(objectClass=group)(member=%{Ldap-
UserDn}))
        Group Member Attr      : radiusGroupName
        Net timeout            : 1 second(s)

Secondary LDAP

        IP Address             : 10.10.10.5
        Port                   : 369
        Login                  :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
        Bind DN                :
cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                : ou=symbol,dc=activedirectory,dc=com
```

```
        Password                : 0 symbol@123
        Password Attribute      : UserPassword
        Group Name              : cn
        Group Membership Filter: (&(objectClass=group)(member=%{Ldap-
UserDn}))
        Group Member Attr       : radiusGroupName
        Net timeout             : 1 second(s)
```

2.2.10 licenses

Common to all modes

Syntax

```
show licenses
```

Parameters

None.

Example

```
WS5100(config)#show licenses
  feature usage    license string                license value     usage
    AP               2FFD7fE9 CD016155 14A92C70              48      1
```

2.2.11 logging

▶ *Common to all modes*

Syntax

```
show logging
```

Parameters

None.

Example

```
WS5100(config)#show logging

Logging module: enabled
    Aggregation time: disabled
    Console logging: level debugging
    Buffered logging: level informational
    Syslog logging: level debugging
        Facility: local7
        Logging to: 157.235.203.37
        Logging to: 10.0.0.2

Log Buffer (6520 bytes):

Sep 14 19:11:59 2006: %DAEMON-6-INFO: radiusd[4643]: Ready to process
requests.

Sep 14 19:11:58 2006: %PM-5-PROCSTOP: Process "radiusd" has been stopped

Sep 14 18:51:14 2006: %CC-5-RADIOADOPTED: 11a radio on AP 00-A0-F8-BF-8A-
A2
adopted

Sep 14 18:51:14 2006: %CC-5-RADIOADOPTED: 11bg radio on AP 00-A0-F8-BF-8A-
A2
adopted
```

2.2.12 mac

Common to all modes

Syntax

```
show mac(access-list)
```

Parameters

access-list	List MAC access lists

Example

2.2.13 management

▶ *Common to all modes*

Syntax

```
show management
```

Parameters

None.

Example

```
WS5100>show management
Mgmt Interface: vlan1
WS5100>
```

2.2.14 mobility

Common to all modes

Syntax

```
show mobility (forwarding | global | mu (AA-BB-CC-DD-EE-FF | detail)|
mu-log | mu-statistics(AA-BB-CC-DD-EE-FF) | peer ( A.B.C.D | detail)| peer-
log)
```

Parameters

mobility	Display Mobility Parameters
forwarding	Display MU Info in the forwarding plane
global	Global Mobility parameters
mu	Mobility MUs
AA-BB-CC-DD-EE-FF	MAC address of the MU
detail	Detailed information display
mu-log	Display Mobility MU Event Log
mu-statistics	Display Mobility MU Stats
AA-BB-CC-DD-EE-FF	MAC address of the MU
peer	Display Mobility peers
A.B.C.D	IP address of Peer
detail	Detailed information display
peer-log	Display Mobility Peer Event Log

Example

```
WS5100(config)#show mobility ?
  event-log    Event Log
  forwarding   Mobile-unit information in the forwarding plane
  global       Global Mobility parameters
  mobile-unit  Mobile-units in the Mobility Database
  peer         Mobility peers
  statistics   Mobile-unit Statistics

WS5100(config)#show mobility event-log mobile-unit
Time            Event        Evt-Src-IP      MU-Mac             MU-IP
HS-IP           CS-IP
09/14 19:17:52  IP-UPD-MU    n/a             00-0f-3d-e9-a6-54
157.235.208.134 157.235.208.16  157.235.208.16
09/14 19:17:51  ADD-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16
09/14 19:17:51  DEL-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16
09/14 19:17:50  ADD-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16

WS5100>show mobility forwarding
Mac-Address        IP-Address       State       Tunnel             HS-Vlan
WS5100>

WS5100>show mobility global
Mobility Global Parameters
Admin-Status                     : DISABLED
Operational-Status               : DISABLED (Admin-status is DISABLED)
Local-Address                    : 0.0.0.0
Max-Roam-Period                  : 5 sec
Number of Peers                  : 0 (established=0)
Number of MUs                    : 0 (Home=0, Foreign=0, Delete-pend=0)
L3-Mobility enabled WLANs        : NONE
WS5100>

WS5100(config)#show mobility mobile-unit detail
HOME MU Database: Total=1
MU MAC-Address: 00-0f-3d-e9-a6-54, IP-Address: 157.235.208.134,
SSID=wios_rad_test1
  Home-Switch: 157.235.208.16, Current-Switch: 157.235.208.16, HS-VLAN=1

Foreign MU Database: Total=0
```

```
WS5100(config)#show mobility peer detail
Mobility Peers: Total=1, Established=0
Peer: 1.1.1.1, State: PASSIVE-CONNECTING
  Join-Sent  : 0      Join-Rcvd  : 0      Leave-Sent : 0      Leave-Rcvd :
0
  Rehome-Sent: 0      Rehome-Rcvd: 0      L3roam-Sent: 0      L3roam-Rcvd:
0
  Num-flaps  : 0      Connect-retries: 0    Peer-Uptime: 0 days, 00:00:00

WS5100(config)#show mobility statistics

MU <00-0f-3d-e9-a6-54> Mob-State HS_AND_CS
-------------------------------------------
Inter-          |Rx                                          |Tx
face            |unicast    MC         BC         Error     |unicast    MC
BC         Error
wlan_port        0          0          0          0          0          0
0          0
```

2.2.15 ntp

▶ *Common to all modes*

Syntax

```
show ntp (association (detail)|status)
```

Parameters

ntp	Network time protocol
association	NTP associations
detail	Displays NTP association details.
status	Displays NTP status.

Example

```
WS5100>show ntp associations
  address         ref clock       st  when  poll  reach  delay  offset
disp
 * master (synced), # master (unsynced), + selected, - candidate, ~
configured
WS5100>

WS5100>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision
is 2**0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
WS5100>

WS5100(config)#show ntp associations detail
157.235.208.105 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
our mode client, peer mode unspec, our poll intvl 6, peer poll intvl 10
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-20,
org time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
rcv time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
xmt time c8b42a7e.6eb04252 (Sep 14 19:22:38 UTC 2006)
filtdelay =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filtoffset =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filterror =  16000.00  16000.00  16000.00  16000.00  16000.00  16000.00
16000.00  16000.00
```

```
WS5100(config)#show ntp status
Clock is unsynchronized, stratum 16, reference is INIT
actual frequency is 0.0000 Hz, precision is 2**-20
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 1395.000 msec,
```

2.2.16 privilege

▶ *Common to all modes*

Syntax

```
show privilege
```

Parameters

None.

Example

```
WS5100>show privilege
Current user privilege: superuser
WS5100>
```

2.2.17 radius

▶ *Common to all modes*

Syntax

```
show radius (configuration | eap (configuration)| group | nas ( A.B.C.D/M)|
proxy | rad-user | trust-point)
```

Parameters

radius	Radius configuration commands
configuration	radius server configuration parameters
eap	Eap parameters
configuration	Eap configuration
group	Radius group configuration
nas	client information
A.B.C.D/M	client ip address / mask
proxy	proxy information
rad-user	Radius user information
trust-point	Radius trust-point configuration

Example

```
WS5100(config)#show radius proxy
Proxy Details

_____________
Proxy retry delay : 6  seconds
Proxy retry count : 4

Proxy Realm Details

____________________
Realm   : symbol.com
        IP Address    : 10.10.10.5
        Port          : 1812
        Shared secret : 0 secret123
```

2.2.18 redundancy-group

▶ *Common to all modes*

Syntax

```
show redundancy-group (config | runtime)
```

Parameters

config	Display configured redundancy group information.
runtime	Display runtime redundancy group information

Example

```
WS5100>show redundancy-group config

Redundancy Group Configuration Detail
Redundancy Feature                  : Disabled
Redundancy group ID                 : 1
Redundancy Mode                     : Primary
Redundancy Interface IP             : 0.0.0.0
Number of configured peer(s)        : 0
Heartbeat-period                    : 5 Seconds
Hold-period                         : 15 Seconds
Discovery-period                    : 30 Seconds
Handle STP                          : Disabled
Switch Installed License            : 0
Switch running image version        : 3.0.0.0-200B
WS5100>

WS5100>show redundancy-group runtime

Redundancy Group Runtime Information
Redundancy Protocol Version          : 2.0
Redundancy Group License             : 0
Cluster AP Adoption Count            : Not Applicable
Switch AP Adoption Count             : Not Applicable
Redundancy State                     : Disabled
Radio Portals adopted by Group       : Not Applicable
Radio Portals adopted by this Switch : Not Applicable
Rogue APs detected in this Group     : Not Applicable
Rogue APs detected by this Switch    : Not Applicable
MUs associated in this Group         : Not Applicable
MUs associated in this Switch        : Not Applicable
Radios in selfhealing mode           : Not Applicable
Selfhealing APs in this Switch       : Not Applicable
Group maximum AP adoption capacity   : Not Applicable
```

```
Switch Adoption capacity             : Not Applicable
Established Peer(s) Count            : Not Applicable
Redundancy Group Connectivity status : Not Applicable

WS5100>

WS5100(config)#show redundancy-group

Redundancy Group Configuration Detail
Redundancy Feature                 : Enabled
Redundancy group ID                : 1
Redundancy Mode                    : Primary
Redundancy Interface IP            : 10.10.10.10
Number of configured peer(s)       : 1
Heartbeat-period                   : 5 Seconds
Hold-period                        : 15 Seconds
Discovery-period                   : 30 Seconds
Handle STP                         : Disabled
Switch Installed License           : 48
Switch running image version       : 3.0.0.0-19635X

Redundancy Group Runtime Information
Redundancy Protocol Version          : 2.0
Redundancy Group License             : 48
Cluster AP Adoption Count            : 1
Switch AP Adoption Count             : 1
Redundancy State                     : Discovery
Radio Portals adopted by Group       : 2
Radio Portals adopted by this Switch : 2
Rogue APs detected in this Group     : 0
Rogue APs detected by this Switch    : 0
MUs associated in this Group         : 1
MUs associated in this Switch        : 1
Selfhealing APs in this Group        : 0
Selfhealing APs in this Switch       : 0
Group maximum AP adoption capacity   : 48
Switch Adoption capacity             : 48
Established Peer(s) Count            : 0
Redundancy Group Connectivity status : Not all members connected
```

2.2.19 redundancy-history

Common to all modes

Syntax

```
show redundancy-history
```

Parameters

None.

Example

```
WS5100>show redundancy-history
State Transition History

Time                        Event Triggered       State
-----------------------------------------------------------

Sep 06 18:20:56 2006        Redundancy Disabled   Disabled

WS5100>
```

2.2.20 redundancy-members

Common to all modes

Syntax

```
show redundancy-members (A.B.C.D)
```

Parameters

A.B.C.D	IP address of member switch

Example

```
WS5100(config)#show redundancy-members brief

Member ID (Self)              : 10.10.10.10
Member State                  : Not Applicable

Member ID                     : 10.10.10.1
Member State                  : Peer Configured
```

2.2.21 snmp

▶ *Common to all modes*

Syntax

```
show snmp (user(manager | operator))
```

Parameters

user	Displays the SNMP user.
manager	show manager information.
operator	show operator information.

Example

```
WS5100>show snmp user manager
userName      access     engineId                Authentication
Encryption
snmpmanager   ro         80000184017f000001      MD5                 DES
snmpoperator  ro         80000184017f000001      MD5                 DES
WS5100>

WS5100>show snmp user operator
userName      access     engineId                Authentication
Encryption
snmpmanager   ro         80000184017f000001      MD5                 DES
snmpoperator  ro         80000184017f000001      MD5                 DES
WS5100>
```

2.2.22 snmp-server

Common to all modes

Syntax

```
show snmp-server(traps(wireless-statistics( mobile-unit | radio |
wireless-switch | wlan)))
```

Parameters

traps	Display Trap enable flags
wireless-statistics	Display wireless-stats rate traps
mobile-unit	Display mobile-unit rate traps
radio	Display radio rate traps
wireless-switch	Display wireless-switch rate traps
wlan	Display wlan rate traps

Example

```
WS5100>show snmp-server traps
------------------------------------------------------------------------
Global enable flag for Traps                                        N
------------------------------------------------------------------------
Enable flag status for Individual Traps
------------------------------------------------------------------------
Module Type               Trap Type                 Enabled?[Y/N]
------------------------------------------------------------------------
snmp                     coldstart                              N
snmp                     linkdown                               N
snmp                     linkup                                 N
snmp                     authenticationFail                     N
nsm                      dhcpIPChanged                          N
redundancy               memberUp                               N
redundancy               memberDown                             N
redundancy               memberMisConfigured                    N
redundancy               adoptionExceeded                       N
redundancy               grpAuthLevelChanged                    N
misc                     lowFsSpace                             N
misc                     processMaxRestartsReached              N
wireless station         associated                             N
wireless station         disassociated                          N
wireless station         deniedAssociationOnCapability          N
wireless station         deniedAssociationOnShortPream          N
```

```
wireless station         deniedAssociationOnSpectrum            N
wireless station         deniedAssociationOnErr                 N
wireless station         deniedAssociationOnSSID                N
wireless station         deniedAssociationOnRates               N
wireless station         deniedAssociationOnInvalidWPAWPA2IE    N
wireless station         deniedAssociationAsPortCapacityReached N
wireless station         tkipCounterMeasures                    N
wireless station         deniedAuthentication                   N
wireless station         radiusAuthFailed                       N
wireless radio           adopted                                N
wireless radio           unadopted                              N
wireless radio           detectedRadar                          N
wireless ap-detection    externalAPDetected                     N
wireless self-healing    activated                              N
wireless ids             excessiveAuthAssociation               N
wireless ids             excessiveProbes                        N
misc                     savedConfigModified                    N
WS5100>

WS5100>show snmp-server traps wireless-statistics mobile-unit
     pktsps-greater-than                    disabled
     tput-greater-than                      disabled
     avg-bit-speed-less-than                disabled
     avg-signal-less-than                   disabled
     nu-percent-greater-than                disabled
     gave-up-percent-greater-than           disabled
     avg-retry-greater-than                 disabled
     undecrypt-percent-greater-than         disabled
WS5100>

WS5100>show snmp-server traps wireless-statistics radio
     pktsps-greater-than                    disabled
     tput-greater-than                      disabled
     avg-bit-speed-less-than                disabled
     avg-signal-less-than                   disabled
     nu-percent-greater-than                disabled
     gave-up-percent-greater-than           disabled
     avg-retry-greater-than                 disabled
     undecrypt-percent-greater-than         disabled
     num-stations-greater-than              disabled
WS5100>

WS5100>show snmp-server traps wireless-statistics wireless-switch
     pktsps-greater-than                    disabled
     tput-greater-than                      disabled
     num-stations-greater-than              disabled
WS5100>
```

```
WS5100>show snmp-server traps wireless-statistics wlan
     pktsps-greater-than                        disabled
     tput-greater-than                          disabled
     avg-bit-speed-less-than                    disabled
     avg-signal-less-than                       disabled
     nu-percent-greater-than                    disabled
     gave-up-percent-greater-than               disabled
     avg-retry-greater-than                     disabled
     undecrypt-percent-greater-than             disabled
     num-stations-greater-than                  disabled
WS5100>
```

2.2.23 terminal

▶ *Common to all modes*

Syntax

```
show terminal
```

Parameters

None.

Example

```
WS5100>show terminal
Terminal Type: vt102
Length: 44     Width: 125
WS5100>
```

2.2.24 timezone

Common to all modes

Syntax

```
show timezone
```

Parameters

None.

Example

```
WS5100>show timezone
Timezone is Etc/UTC
WS5100>
```

2.2.25 users

Common to all modes

Syntax

```
show users
```

Parameters

None.

Example

```
WS5100>show users
   Line       PID   User        Uptime      Location
   0 con 0  306               6d07h11m     ttyS0
 130 vty 0  1961               02:51:45     0
WS5100>
```

2.2.26 version

Common to all modes

Syntax

```
show version (verbose)
```

Parameters

verbose	Display software & hardware details

Example

```
WS5100>show version
WS5100 version 3.0.0.0-200B
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.

Switch uptime is 6 days, 7 hours 23 minutes
CPU is Intel(R) Pentium(R) 4 CPU 2.00GHz
256220 kB of on-board RAM
ide device hda disk model Kouwell DOM capacity 501760 blocks, cache 0
WS5100>

WS5100>show version verbose
WS5100 version 3.0.0.0-200B
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.

Switch uptime is 6 days, 7 hours 22 minutes
CPU is Intel(R) Pentium(R) 4 CPU 2.00GHz
256220 kB of on-board RAM
ide device hda disk model Kouwell DOM capacity 501760 blocks, cache 0
Failed to open /proc/pci for input
WS5100>
```

2.2.27 wireless

▶ *Common to all modes*

Syntax

```
show wireless (ap (<1-48>|AA-BB-CC-DD-EE-FF)| ap-detection-config | ap-images
| ap-unadopted | approved-aps | channel-power (11a (indoor | outdoor))|
11b (indoor | outdoor)| 11bg (indoor | outdoor))| config | hotspot-config
<1-32>| ids (filter-list)|mac-auth-local<1-1000> | mobile-unit(<1-4096> |
AA-BB-CC-DD-EE-FF | statistics) | phrase-to-key (wep128 | wep64)| qos-mapping
(wired-to-wireless | wireless-to-wired)| radio ( <1-1000> | beacon-table |
config ( <1-1000> |default-11a |default-11b | default-11bg)| monitor-table
| statistics)( <1-1000> | beacon-table | config | monitor-table |
statistics)|regulatory (country codes)| self-heal-config <1-1000>| sensor
(default-config | discovered-sensors)| unapproved-aps | wireless-switch-
statistics (detail)| wlan ((config( <1-32> | all | enabled)| statistics <1-
32>))

show wireless ap (<1-48>|AA-BB-CC-DD-EE-FF)
show wireless ap-detection-config
Show wireless ap-images
show wireless ap-unadopted
show wireless approved-aps
show wireless channel-power (11a (indoor | outdoor)| 11b (indoor |
                             outdoor)| 11bg indoor | outdoor))
show wireless config
show wireless hotspot-config <1-32 >
show wireless ids (filter-list)
show wireless mac-auth-local<1-1000>
show wireless mobile-unit (<1-4096> | AA-BB-CC-DD-EE-FF | statistics)
show wireless phrase-to-key (wep128 | wep64)
show wireless qos-mapping (wired-to-wireless | wireless-to-wired)
show wireless radio ( <1-1000> | beacon-table | config ( <1-1000> |
                      default-11a |default-11b | default-11bg)|
                       monitor-table | statistics)
show wireless regulatory (country codes)
show wireless self-heal-config <1-1000>
show wireless sensor (default-config | discovered-sensors)
show wireless unapproved-aps
show wireless wireless-switch-statistics (detail)
show wireless wlan (config( <1-32> | all | enabled)| statistics <1-32>)
```

Parameters

ap	Status of adopted access-port
<1-48>	The index of the access-port for detailed information
AA-BB-CC-DD-EE-FF	The MAC address of a access-port for detailed information
ap-detection-config	Detected-AP Configuration Parameters
ap-images	List of access-port images on the wireless switch
ap-unadopted	List of unadopted access-port
approved-aps	Approved APs seen by access-port scans
channel-power	List of available channel and power levels for a radio
11a	radio is of type 802.11a
11b	radio is of type 802.11b
11bg	radio is of type 802.11bg
indoor	radio is placed indoor
outdoor	radio is placed outdoor
config	Wireless Configuration Parameters
hotspot-config	Wlan hotspot configuration
<1-32>	A wlan index <1-32>
ids	Intrusion detection parameters
filter-list	Display the list of currently filtered mobile-units
mac-auth-local	list out the mac-auth-local entries
<1-1000>	mac-auth-local entry to display
mobile-unit	Details of associated mobile-units
<1-4096>	Index of mobile-unit

AA-BB-CC-DD-EE-FF	MAC address of mobile-unit
statistics	mobile-unit rf statistics
phrase-to-key	display the WEP keys generated by a passphrase
wep128	display WEP128 keys
wep64	display WEP64 keys
qos-mapping	Quality of Service mappings used for mapping WMM access categories and 802.1p / DSCP tags.
wired-to-wireless	Mappings used when traffic is switched from wired to the wireless side.
wireless-to-wired	Mappings used when traffic is switched from wireless to the wired side.
radio	Radio related commands
<1-1000>	A single radio index
beacon-table	The Radio-to-Radio beacon table
config	Radio configuration
<1-1000>	A single radio index
default-11a	default 11a configuration template
default-11b	default 11b configuration template
default-11bg	default 11bg configuration template
monitor-table	The Radio-to-Radio monitoring table
statistics	Radio statistics
regulatory	Regulatory (allowed channel/power) information for a particular country.
self-heal-config	Self-Healing Configuration Parameters
<1-1000>	A single radio index
all	All Configured radios
sensor	Wireless Intrusion Protection System parameters

default-config	Default configuration parameters for sensors
discovered-sensors	sensor access ports discovered by the switch
unapproved-aps	Unapproved APs seen by access-port or mobile-unit scans
wireless-switch-statistics	wireless-switch statistics
detail	Detailed wireless-switch statistics
wlan	Wireless LAN related parameters
config	Wlan configuration
<1-32>	A wlan index <1-32>
all	All wlans in configuration
enabled	Only wlans that are currently enabled
statistics	WLAN statistics
<1-32>	A wlan index <1-32>

Example

```
WS5100>show wireless ap
Number of access-ports adopted   : 0
Available licenses               : 0
Clustering enabled               : N
Clustering mode                  : primary
WS5100>

WS5100>show wireless ap-detection-config
max-detected-aps         : 100
mu-assisted scan         : disabled
mu-assisted scan refresh : 1800 seconds
configured approved-aps  :
Index | Bss Mac           | Ssid
-----------------------------------------------------
WS5100>

WS5100>show wireless ap-images
  Idx   ap-type      Image-Name         Size (bytes)  Version
   1    ap300     WISP-AP300              293516      00.02-29
   2    ap300     WIAP-300                244076      01.00-1635b
```

```
   3    ap300     AP300-IDS-Sensor        295064      00.00-04
   4    ap100     AP100                   31034       02.05-00
   5    ap4131    AP4131                  191440      07.00-01
   6    ap4131    Revert-AP4131           665704      00.00-00
WS5100>

WS5100>show wireless ap-unadopted
WS5100>

WS5100>show wireless approved-aps
access-port detection is disabled
WS5100>

WS5100>show wireless channel-power 11a indoor
% Error: No valid channels or power levels
WS5100>

WS5100>show wireless config
country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
dot11-shared-key-auth   : disabled
ap-detection            : disabled
oversized-frames        : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp fix windows        : disabled
broadcast-tx-speed      : optimize-for-throughput
smart-scan 11a channels :
smart-scan 11bg channels:
WS5100>

WS5100>show wireless hotspot-config

WLAN: 1 status: disabled description: WLAN1 ssid: 101
 Page-Location: simple
 Internal Pages
  Page-type : login
   Title : Login Page
   Header : Network Login
   Description : Please enter your username and password
   Footer : Contact the network administrator if you do not have an
account
  Image URL main:
  Image URL small:

  Page-type : welcome
   Title : Authentication success.
```

```
   Header : Authentication Success.
   Description : You now have network access.<BR>Click the disconnect link
below to end this session.
   Footer :
  Image URL main:
  Image URL small:

  Page-type : fail
   Title : Unable to authenticate
   Header : Authentication Failed.
   Description : Either the username and password are invalid, or service
is unavailable at this time
   Footer : Contact the network administrator if you do not have an
account
  Image URL main:
  Image URL small:

 External Pages
  Page-Type : login
   URL :
  Page-Type : welcome
   URL :
  Page-Type : fail
   URL :
Allow-list IP addresses

WLAN: 2 status: disabled description: WLAN2 ssid: 102
 Page-Location: simple
 Internal Pages
  Page-type : login
   Title : Login Page
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
................................................

WS5100>show wireless ids
 detect-window               : 10 seconds

 Excessive Operations::  Threshold(mu radio switch)   Filter-Ageout
  probe-requests       :       0      0      0             60 Sec
  association-requests :       0      0      0             60 Sec
  disassociations      :       0      0      0             60 Sec
  authentication-fails :       0      0      0             60 Sec
  crypto-replay-fails  :       0      0      0             60 Sec
  80211-replay-fails   :       0      0      0             60 Sec
  decryption-fails     :       0      0      0             60 Sec
  unassoc-frames       :       0      0      0             60 Sec
  eap-starts           :       0      0      0             60 Sec
```

```
 Anomaly Detection::              Status     Filter-Ageout
  probe-requests           :   disabled      60 Sec
  association-requests     :   disabled      60 Sec
  disassociations          :   disabled      60 Sec
  authentication-fails     :   disabled      60 Sec
  crypto-replay-fails      :   disabled      60 Sec
  80211-replay-fails       :   disabled      60 Sec
  decryption-fails         :   disabled      60 Sec
  unassoc-frames           :   disabled      60 Sec
  eap-starts               :   disabled      60 Sec
  null-destination         :   disabled      60 Sec
  same-source-destination  :   disabled      60 Sec
  multicast-source         :   disabled      60 Sec
  weak-wep-iv              :   disabled      60 Sec
  tkip-countermeasures     :   disabled      60 Sec
  invalid-frame-length     :   disabled      60 Sec
WS5100>

WS5100>show wireless mac-auth-local 50
WS5100>

WS5100>show wireless mobile-unit statistics
% Error: None of the mobile-units are associated!!
```

2.2.28 access-list

Priviledge / Global Config

This CLI command lists all the access lists (numbered and named) configured on the switch. The numbered access list displays all numbered ACLs configured and the named access-list displays the details of the name ACL configured.

Syntax

```
show access-list
show access-list ( <1-99> | <100-199> | <1300-1999> | <2000-2699> | WORD )
Show access-list <acl-name>
```

Parameters

<1-99>	IP standard access list
<100-199>	IP extended access list
<1300-1999>	IP standard access list (expanded range)
<2000-2699>	IP extended access list (expanded range)
WORD	Name of ACL

Example

2.2.29 alarm-log

▶ *Priviledge / Global Config*

Syntax

```
show alarm-log ( <1-65535>| acknowledged | all | count | new |
severity-to-limit( critical |informational | major | normal | warning))
```

Parameters

<1-65535>	Display details for specific alarm id
acknowledged	Display acknowledged alarms currently in the system
all	Display all alarms currently in the system
count	Display count of alarms currently in the system
new	Display new alarms currently in the system
severity-to-limit	Display all alarms having specified or higher severity
critical	Display all critical alarms
informational	Display all informational or higher severity alarms
major	Display all major or higher severity alarms
normal	Display all normal or higher severity alarms
warning	Display all warning or higher severity alarms

Example

2.2.30 boot

Priviledge / Global Config

Syntax

```
show boot
```

Parameters

None.

Example

```
WS5100#show boot

Image           Build Date              Install Date           Version
-----       --------------------    --------------------      ------------
--
Primary     Aug 28 14:05:16 2006     Aug 29 18:32:17 2006     3.0.0.0-200B
Secondary   Aug 14 06:18:03 2006     Aug 17 15:08:28 2006     3.0.0.0-180B

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
WS5100#
```

2.2.31 clock

▶ *Priviledge / Global Config*

Syntax

```
show clock
```

Parameters

None.

Example

```
WS5100#show clock
Sep 13 16:46:27 UTC 2006
WS5100#
```

2.2.32 debugging

Priviledge / Global Config

Syntax

```
show debugging
```

Parameters

None.

Example

2.2.33 file

▶ *Privilege / Global Config*

Syntax

```
show file (information (FILE)| systems)
```

Parameters

information	Display file information
FILE	Display information on FILE
systems	List filesystems

Example

```
WS5100#show file systems
File Systems:

     Size(b)     Free(b)     Type  Prefix
           -           -   opaque  system:
    13704192    11904000    flash  nvram:
    19524608    16866304    flash  flash:
           -           -  network  sftp:
           -           -  network  http:
           -           -  network  ftp:
           -           -  network  tftp:
WS5100#
```

2.2.34 ftp

Privilege / Global Config

Syntax

```
show ftp
```

Parameters

None.

Example

```
WS5100#show ftp
FTP Server: Disabled
User Name:  anonymous or ftpuser
Password:   ********
Root dir:   flash:/
WS5100#
```

2.2.35 password-encryption

▶ *Priviledge / Global Config*

Syntax

```
show password-encryption (status)
```

Parameters

status	Display password-encryption status

Example

```
WS5100#show password-encryption status
Password encryption is disabled
WS5100#
```

2.2.36 running-config

Privilege / Global Config

Displays the contents of the configuration file for the switch including all configured MAC and IP access lists and which access groups are applied to an interface.

Syntax

```
show running-config(full|include-factory)
```

Parameters

full	full configuration
include-factory	Include Factory Defaults

Example

```
WS5100#show running-config full
!
! configuration of WS5100 version 3.0.0.0-200B!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username manager privilege  superuser
!
!
no country-code
logging console 7
no logging on
fallback enable
ftp password 1 810a25d76c31e495cc070bdf42e076f7c9b0a1cd
ip http server
ip http secure-trustpoint local
ip http secure-server
ip ssh
ip telnet
snmp-server manager v2
snmp-server manager v3
crypto isakmp identity address
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
!
```

```
wireless
!
crypto pki trustpoint local
 subject-name 11 11 11 11 11 11
crypto pki trustpoint default-trustpoint
 subject-name Symbol Technologies
crypto pki trustpoint slocal
!
radius-server local
!
interface eth1
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
.................................................

WS5100#show running-config include-factory
!
! configuration of WS5100 version 3.0.0.0-200B!
version 1.0
!
no service password-encryption
service prompt crash-info
no service set command-history
no service set reboot-history
no service set upgrade-history
!
hostname WS5100
!
banner motd Welcome to CLI
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin access  console snmp ssh telnet
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username operator access  console snmp ssh telnet
username operator privilege  monitor
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username manager access  console snmp ssh telnet
username manager privilege  superuser
!
!
ip domain-lookup
service pm max-sys-restarts 2
no service pm sys-restart
service diag period 1000
service diag enable
no country-code
redundancy group-id 1
redundancy interface-ip 0.0.0.0
redundancy mode primary
```

```
redundancy heartbeat-period 5
redundancy hold-period 15
redundancy discovery-period 30
no redundancy handle-stp enable
no redundancy enable
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
.............................................
```

2.2.37 securitymgr

▶ *Privilege / Global Config*

Syntax

```
show securitymgr(debug-logs)
```

Parameters

debug-logs	Debug information

Example

2.2.38 sessions

Privilege / Global Config

Syntax

```
show sessions
```

Parameters

None.

Example

```
WS5100#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
   1       cli    Console           006days     Jan  1 00:00:00 1970
** 2       cli    157.235.206.39    00:00m      Jan  1 00:00:00 1970
WS5100#
```

2.2.39 startup-config

▶ *Privilege / Global Config*

Syntax

```
show startup-config
```

Parameters

None.

Example

```
WS5100#show startup-config
!
! configuration of WS5100 version 3.0.0.0-16786X!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username manager privilege  superuser
!
!
!
!
no country-code
logging console 7
no logging on
fallback enable
ftp password 1 810a25d76c31e495cc070bdf42e076f7c9b0a1cd
ip http server
ip http secure-trustpoint local
ip http secure-server
ip ssh
ip telnet
snmp-server manager v2
snmp-server manager v3
snmp-server user manager v3 encrypted auth md5
0xfdcea1ff2d738d4bf1bc072f0d6094b7
snmp-server user operator v3 encrypted auth md5
0xfb2392a14cf80787b878006ab968a29b
crypto ipsec security-association lifetime kilobytes 4608000
!
wireless
!
crypto pki trustpoint slocal.................................
```

2.2.40 upgrade-status

Privilege / Global Config

Syntax

```
show upgrade-status(detail)
```

Parameters

detail	Last image upgrade log

Example

```
WS5100#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Aug 29 18:32:17 2006
-------------------------------------------------------
var2 is 10 percent full
/tmp is 5 percent full
Free Memory 151944 kB
FWU invoked via Linux shell
Running from partition /dev/hda6, partition to update is /dev/hda5
Reading image file header
Removing other partition
Added 3.0.0.0-180B *
Making file system
Extracting files (this can take some time).
Version of firmware update file is 3.0.0.0-200B
Creating LILO files
Running LILO
Added 3.0.0.0-180B *
Added 3.0.0.0-200B
Successful
WS5100#
```

3

User Exec Commands

Logging in to the switch places you in USER EXEC command mode. Typically, log-in will require a user name and a password. You may try three times to enter a password before the connection attempt is refused.The USER EXEC commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC commands allow you to connect to remote devices, perform basic tests, and list system information.

To list the available USER EXEC commands, use the **?** at the command prompt. The USER EXEC mode prompt consists of the host name of the device followed by an angle bracket (**>**). The default host name is generally WLAN Module. You can change the host name using the hostname GLOBAL CONFIG command.

3.1 User Exec Commands

Table 3.1 summarizes the User Exec commands within the WS5100 Series Switch command line interface.

Table 3.1 User Exec commands Summary

Command	Description	Ref.
autoinstall	autoinstall configuration command.	page 3-3
clear	autoinstall configuration command.	page 3-4
clrscr	the display screen.	page 2-3
cluster-cli	Cluster context.	page 3-6
debug	Debugging functions.	page 3-7
disable	Turn off privileged mode command.	page 3-9
enable	Turn on privileged mode command.	page 3-10
exit	End current mode and down to previous mode.	page 2-4
help	Description of the interactive help system.	page 2-5
logout	Exit from the EXEC.	page 3-11
no	Negate a command or set its defaults.	page 2-7
page	Toggle paging.	page 3-12
quit	Exit current mode and down to previous mode.	page 3-13
service	Service Commands.	page 2-8
terminal	Show running system information.	page 2-19

3.1.1 autoinstall

User Exec Commands

Use this command to configure the auto -install feature of the WS5100 Series Switch.

Syntax

```
autoinstall start
autoinstall (config|cluster-config|image) url LINE
```

Parameters

enable	Enables all the autoinstall features.

Usage Guidelines

Example

```
WS5100>autoinstall enable
WS5100>
```

3.1.2 clear

User Exec Commands

Use this command to reset the prevoius command implemented by you.

Syntax

```
clear (crypto (ike sa ( A.B.C.D| )|ipsec sa(A.B.C.D | ) )|
mobility(mu|mu-log|peer-log|peer-statistics)| wireless-statistics )
```

Parameters

crypto	crypto
mobility	Clear Mobility Attributes
wireless-statisitcs	Clear all wireless statistics
ike	
ipsec	
sa	Security association
remote peer IP address	IP address of the remote peer
peer IP address	IP addres of the peer
mu	Clear Mobile-unit
AA-BB-CC-DD-EE-FF	MAC address of the MU
all	All MUs (Home and Foreign)
foreign-database	MUs present in the Foreign MU Database
home-database	MUs present in the Home MU Database
mu-log	Clear Mobility MU-Event Log
peer-log	Clear Mobility PEER-Event Log
peer-statisitcs	Clear Mobility Peer Statistcs
A.B.C.D	IP address of the peer

Usage Guidelines

Example

```
WS5100>clear crypto ike sa 111.222.333.01
WS5100>

WS5100>clear crypto ipsec sa
WS5100>
```

3.1.3 cluster-cli

▶ *User Exec Commands*

Use this command to cluster all the CLI pertaining to the context it appears in.

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables cluster context

Usage Guidelines

Example

```
WS5100>cluster-cli enable
WS5100>
```

3.1.4 debug

User Exec Commands

Use this command to debug the WS5100 Series Switch.

Syntax

```
debug (certmgr(all|err|info)|ip ssh|
       mobility(cc|error|forwarding|mu|packet|peer|system))
```

Parameters

certmgr	Certificate Manager Debugging Messages
ip	Internet Protocol (IP)
mobility	L3 Mobility
all	Trace error and informational messages from Certificate Manager
error	Trace error messages from Certificate Manager
info	Trace informational messages from Certificate Manager
ssh	Secured Shell (SSH) server
cc	ccserver events
error	Error
forwarding	Dataplane forwarding
mu	MU events and state changes
packet	Control Packets
peer	Peer establishment
system	System events

Usage Guidelines

Example

```
WS5100>debug certmgr all
WS5100>

WS5100>debug certmgr error
WS5100>

WS5100>debug certmgr info
WS5100>

WS5100>debug ip ssh
WS5100>

WS5100>debug mobility cc
WS5100>

WS5100>debug mobility error
WS5100>
WS5100>debug mobility forwarding
WS5100>

WS5100>debug mobility mu
WS5100>

WS5100>debug mobility packet
WS5100>

WS5100>debug mobility peer
WS5100>

WS5100>debug mobility system
WS5100>
```

3.1.5 disable

User Exec Commands

To use this command you first have to enable the PRIV mode. Use this command to turn off and move out of the PRIV mode.

Syntax

```
disable
```

Parameters

None.

Usage Guidelines

Example

```
WS5100>disable
WS5100>
```

3.1.6 enable

User Exec Commands

Use this command to enter into the PRIV mode.

Syntax

```
enable
```

Parameters

None.

Usage Guidelines

Example

```
WS5100>enable
```

3.1.7 logout

User Exec Commands

Use this command instead of `exit` command to exit from the EXEC mode.

Syntax

```
logout
```

Parameters

None.

Usage Guidelines

Example

```
The WS5100 Series Switch logs off on execution of this command.
```

3.1.8 page

User Exec Commands

Use this command to toggle paging.

Syntax

page

Parameters

None.

Usage Guidelines

Example

3.1.9 quit

User Exec Commands

Use this command to exit from the current mode and go down to previous mode.

Syntax

```
quit
```

Parameters

None.

Usage Guidelines

Example

```
The WS5100 Series Switch logs off on execution of this command.
```

4

Privileged Exec Commands

Most of the PRIV EXEC mode commands set operating parameters, privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes those commands contained in USER EXEC mode. PRIV EXEC mode also provides access to configuration modes through the configure command, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device followed by a pound sign (**#**). To access PRIV EXEC mode enter the following CLI command at the prompt:

```
WS5100#enable
```

PRIV EXEC mode is sometimes referred to as **enable mode**, because the `enable` command is used to enter the mode.

If a password has been configured on the system, you will be prompted to enter it before being allowed access to privileged EXEC mode. The password is not displayed on the screen and is case sensitive. If an enable password has not been set, PRIV EXEC mode can be accessed only from the router console (terminal connected to the console port). The system administrator uses the enable secret or enable password.

4.1 Priv Exec Command

Table 4.1 summarizes the Priv Exec commands within the WS5100 Series Switch command line interface.

Table 4.1 Priv Exec Command Summary

Command	Description	Ref.
acknowledge	Acknowledge alarms.	page 4-4
archive	Manage archive files.	page 4-5
autoinstall	autoinstall configuration command.	page 4-7
cd	Change current directory.	page 4-8
clear	Reset functions.	page 4-9
clock	Configure software system clock.	page 4-11
clrscr	the display screen.	page 2-3
cluster-cli	Cluster context.	page 4-12
configure	Enter configuration mode.	page 4-13
copy	Copy from one file to another.	page 4-14
debug	Debugging functions.	page 4-15
delete	Deletes specified file from the system.	page 4-16
diff	Display differences between two files.	page 4-17
dir	List files on a filesystem.	page 4-18
disable	Turn off privileged mode command.	page 4-19
edit	Edit a text file.	page 4-20
enable	Turn on privileged mode command.	page 4-22
erase	Erase a filesystem.	page 4-23
exit	End current mode and down to previous mode.	page 2-4
halt	Halt wireless switch.	page 4-24

Command	Description	Ref.
help	Description of the interactive help system.	page 2-5
kill	Kill specified session.	page 4-25
logout	Exit from the EXEC.	page 4-26
mkdir	Create a directory.	page 4-27
more	Display the contents of a file.	page 4-28
no	Negate a command or set its defaults.	page 2-7
page	Toggle paging.	page 4-30
ping	Send ICMP echo messages.	page 4-31
pwd	Display current directory.	page 4-32
quit	Exit current mode and down to previous mode.	page 4-33
reload	Halt and perform a warm reboot.	page 4-34
rename	Rename a file.	page 4-35
rmdir	Delete a directory.	page 4-36
service	Service Commands.	page 2-8
terminal	Show running system information.	page 2-19
telnet	Open a telnet connection.	page 4-37
traceroute	Trace route to destination.	page 4-38
upgrade	Upgrade software image.	page 4-39
upgrade-abort	Abort an ongoing upgrade.	page 4-41
write	Write running configuration to memory or terminal.	page 4-42

4.1.1 acknowledge

Priv Exec Command

Use this command to acknowledge alarms generated by the WS5100 Series Switch.

Syntax

```
acknowledge alarm-log [<1-65535> | all]
```

Parameters

alarm-log	Acknowledge alarms
<1-65535>	Acknowledge specific alarm id
all	Acknowledge all alarms

Example

```
WS5100#acknowledge alarm-log all
No corresponding record found in the Alarm Log.

WS5100#acknowledge alarm-log 200
No corresponding record found in the Alarm Log.
WS5100#
```

4.1.2 archive

▶ *Priv Exec Command*

Use this command to manage archive files.

Syntax

```
archive tar /table [FILE|URL]
archive tar /create [FILE|URL] .FILE
archive tar /xtract [FILE|URL] DIR
```

Parameters

tar	Use to manipulate (create, list or extract) a tar file
`/table`	List files in a tar file
`/create`	Create a tar file
`/xtract`	Extract files from a tar file
`FILE`	Tar filename
`URL`	Tar file URL

Example

How to zip the folder flash:/log/?

```
WS5100#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
WS5100#dir flash:/
```

Viewing the output tar file?

```
Directory of flash:/
  drwx   1024      Thu Aug 17 08:25:50 2006   hotspot
  drwx   120       Fri Sep  8 12:27:20 2006   log
  drwx   1024      Thu Sep  7 16:23:34 2006   crashinfo
  drwx   1024      Wed Aug 23 15:30:19 2006   backup
  -rw-   173056    Fri Sep  8 14:39:48 2006   out.tar
```

Which files are tared?

```
WS5100#archive tar /table flash:/out.tar
drwxrwxrwt 0/600         0 2006-09-08 12:27:20 flash/log
-rw-r--r-- 0/0         381 2006-09-08 12:27:28 flash/log/snmpd.log
-rw-r--r-- 0/0      151327 2006-09-08 14:37:26 flash/log/messages.log
-rw-r--r-- 0/0       17318 2006-09-08 12:27:29 flash/log/startup.log
drwxrwxrwt 0/600         0 2006-09-08 12:27:14 flash/log/radius
```

Untar fails..?

```
WS5100#archive tar /xtract flash:/out.tar flash:/out/
tar: flash:/out.tar: No such file or directory
```

4.1.3 autoinstall

Priv Exec Command

Use this CLI to configure auto-installation feature of the WS5100 Series Switch.

Syntax

```
autoinstall start
autoinstall [config|cluster-config|image] url LINE
```

Parameters

start	start the autoinstall sequence
cluster-config	enable autoinstall of cluster-config
config	enable autoinstall of config
image	enable autoinstall of image

Example

4.1.4 cd

Priv Exec Command

Use this CLI to change the current directory.

Syntax

```
cd [DIR|]
```

Parameters

DIR	Change current directory to DIR.

Usage Guidelines

Example

```
WS5100#cd
nvram:/   system:/  flash:/
WS5100#cd flash:/?
  DIR  Change current directory to DIR
WS5100#cd flash:/
flash:/backup/     flash:/crashinfo/  flash:/hotspot/    flash:/log/
flash:/out/
WS5100#cd flash:/log/?
  DIR  Change current directory to DIR
WS5100#cd flash:/log/
WS5100#pwd
flash:/log/
WS5100#
```

4.1.5 clear

▶ *Priv Exec Command*

Use this CLI to reset the current context.

Syntax

```
clear [alarm-log|arp-cache|crypto|ip|logging|mobility|wireless-statistics]
clear alarm-log (<1-65535>|acknowledge|all|new)
clear crypto(ike|ipsec)sa(remote peer)
clear ip(dhcp(binding)[*|A.B.C.D]|nat(translation)*)
clear mobility(mu|mu-log|peer-log|peer-statistics)
clear mobility mu(<MAC Address>|all|foreign-database|home-database)
```

Parameters

alarm-log	Clear alarm-log • <1-65535> – Clear specific alarm id • acknowledge – Clear acknowledged alarms • all – Clear all alarms • new – Clear new alarms
arp-cache	Clear Arp Cache
crypto	crypto • **ike** – clear ike • **ipsec** – clear ipsec • sa – Security Association • *remote-peer* – Remote Peer IP address
ip	Clears Internet Protocol (IP) DHCP/NAT. • **dhcp** – DHCP Server Configuration • *binding* – DHCP Address bindings • *** – Clear all bindings • *A.B.C.D* – Clear a specific binding • **nat** – Network Address Translation (NAT) • *translation* – Clears specified Translation.
logging	Modify message logging facilities

mobility	Clear Mobility Attributes • **mu** – Clear Mobile-unit • *MAC Address* – MAC address of the MU • *all* – All MUs (Home and Foreign) • *foreign-database* – MUs present in the Foreign MU Database • *home-database* – MUs present in the Home MU Database • **mu-log** – Clear Mobility MU-Event Log • **peer-log** – Clear Mobility PEER-Event Log • **peer-statisitcs** – Clear Mobility Peer Statistcs
wireless-statistics	Clear all wireless statistics

Example

4.1.6 clock

Priv Exec Command

Use this command to configure the software system clock.

Syntax

```
clock set HH:MM:SS [1-31] MONTH [1993-2035]
```

Parameters

set	Set system date & time

Usage Guidelines

Example

```
WS5100#clock set 15:10:30 08 Sep 2006
WS5100#show clock
Sep 08 15:10:31 UTC 2006
```

4.1.7 cluster-cli

Priv Exec Command

Use this CLI command to enable the cluster context.

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables cluster context

Example

4.1.8 configure

Priv Exec Command

Use this CLI to enter into configuration mode.

Syntax

```
configure terminal
```

Parameters

terminal	Configure from the terminal

Usage Guidelines

Example

```
WS5100#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
WS5100(config)#
```

4.1.9 copy

Priv Exec Command

Use this command to copy from one file to another file.

Syntax

```
copy (FILE|URL) (FILE|URL)
```

Parameters

FILE	File from which to copy
URL	URL from which to copy

Usage Guidelines

Example

Transfering file snmpd.log to remote tftp server?

```
WS5100#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into switchrunning-config?

```
WS5100#copy tftp://157.235.208.105:/running-
config running-config
```

4.1.10 debug

Priv Exec Command

Use this CLI for debugging purpose. Apart from `all` this CLI is also used to debug various features of the WS5100 Series Switch.

Syntax

```
debug all
debug [other features]
```

Parameters

all	Enable all debugging

Usage Guidelines

Example

```
WS5100#debug ?
  all                 Enable all debugging
  cc                  Cellcontroller (wireless) debugging messages
  certmgr             Certificate Manager Debugging Messages
  dhcpsvr             DHCP Conf Server Debugging Messages
  imi                 Integrated Management Interface
  ip                  Internet Protocol (IP)
  logging             Modify message logging facilities
  mgmt                Mgmt daemon
  mobility            L3 Mobility
  nsm                 Network Service Module (NSM)
  pktdrvr             Pktdrvr (kernel wireless) debugging messages
  pm                  Process Monitor
  radius              Radius server debugging messages
  redundancy          Redundancy Protocol debugging messages
  securitymgr         Security Manager Debugging Messages
  wireless-statistics  wireless statistics
```

4.1.11 delete

Priv Exec Command

Use this command to delete the specified file from the system.

Syntax

```
delete ({/force|/recursive}|) .FILE
```

Parameters

/force	Force deletion without prompt
/recursive	Recursive delete
FILE	Filename(s) to be deleted

Usage Guidelines

Example

```
WS5100#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

WS5100#delete /force flash:/tmp.txt
WS5100#

WS5100#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
WS5100#
```

4.1.12 diff

▶ *Priv Exec Command*

Use this CLI to view the difference between 2 files.

Syntax

```
diff (FILE|URL) (FILE|URL)
```

Parameters

FILE	Display the differences between FILE
URL	Display the differences between URL

Usage Guidelines

Example

```
WS5100#diff startup-config running-config
--- startup-config
+++ running-config
@@ -89,7 +89,7 @@
  mobility peer 157.235.208.16
  wlan 1 enable
  wlan 1 ssid wlan123
- wlan 1 encryption-type wep128
+ wlan 1 encryption-type tkip
  wlan 1 authentication-type eap
  wlan 1 mobility enable
  wlan 1 radius server primary 127.0.0.1
@@ -184,10 +184,12 @@
  rad-user adam password 0 mypassword
  rad-user eve password 0 mypassword123
  rad-user sumi password 0 mypassword
+ rad-user test password 0 mypassword123
  rad-user vasavi password 0 mypassword123
  group kumar2
   rad-user sumi
-  policy wlan 2
+  policy vlan 44
+  policy wlan 10
  !
  group kumar3
  !
```

4.1.13 dir

▶ *Priv Exec Command*

Use this CLI to view the list of files on a filesystem.

Syntax

```
dir ({/all|/recursive}|) (DIR|all-filesystems|)
```

Parameters

/all	List all files
/recursive	List files recursively
DIR	List files in named file path
all-filesystems	List files on all filesystems
|	Output modifiers
>	Output redirection
>>	Output redirection appending

Usage Guidelines

Example

```
WS5100#dir
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt

WS5100#
```

4.1.14 disable

Priv Exec Command

Use this command to turn off privileged mode command.

Syntax

```
disable
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#disable
WS5100>
```

4.1.15 edit

▶ *Priv Exec Command*

Use this CLI command to edit a text file.

Syntax

```
edit FILE
```

Parameters

FILE	Name of the file to be edited.

Usage Guidelines

Example

```
S5100# edit startup-config
GNU nano 1.2.4               File: startup-config
!
! configuration of WS5100 version 3.0.0.0-
19193X!
version 1.0
!
service prompt crash-info
!
username ksd
username jskdf
username admin password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1
fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1
8e67bb26b358e2ed20fe552ed6fb832f397a507d
username manager privilege  superuser
username test password 1
d11168bcad36bbbdec594be55f5020cf0e086859
username test access  ssh
username test privilege  superuser
!
!
ip access-list extended remote
[ Read 423 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev
Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next
Page ^U UnCut Txt ^T To Spell
```

```
< this command will open the startup-config
file for editing >
< edit & save the config file & exit>
WS5100#
```

4.1.16 enable

Priv Exec Command

Use this CLI command to Turn on privileged mode command.

Syntax

```
enable
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#enable
WS5100#
```

4.1.17 erase

▶ *Priv Exec Command*

Use this CLI command to erase a filesystem.

Syntax

```
erase (nvram:|flash:|startup-config)
```

Parameters

nvram:	Erase everything in nvram:
flash:	Erase everything in flash:
startup-config	Reset configuration to factory default

Usage Guidelines

Example

```
WS5100#erase flash:
% Error: path is a directory
WS5100#erase ne
WS5100#erase nvram:
% Error: no user deleteable files in nvram:
WS5100#erase startup-config
WS5100#
```

4.1.18 halt

Priv Exec Command

Use this CLI command to stop the WS5100 Series Switch.

Syntax

```
halt
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#halt
Wireless switch will be halted, do you want to continue? (y/n): y
.........
```

4.1.19 kill

▶ *Priv Exec Command*

Use this CLI command to kill a specified session.

Syntax

```
kill session <1-16>
```

Parameters

session	Active session. There are 16 active sessions which can be killed

Usage Guidelines

Example

```
Telnet to switch
[xyz@xyz xyz]$ telnet

157.235.208.93
Trying 157.235.208.93...
Connected to 157.235.208.93 (157.235.208.93).
Escape character is '^]'.

WS5100 release 3.0.0.0-19193X
Login as 'cli' to access CLI.
WS5100 login: root
~ #
WS5100#show sessions
SESSION   USER       LOCATION        IDLE

  START TIME
** 1       root   Console           00:00m

Jan  1 00:00:00 1970
   2       root   157.235.208.105   00:38m

Jan  1 00:00:00 1970
   3       root   157.235.208.105   00:00m

Jan  1 00:00:00 1970
WS5100#kill session 9
% Error: Invalid session number
WS5100#kill session 3

~ # Connection closed by foreign host.
[xyz@xyz xyz]$
```

4.1.20 logout

Priv Exec Command

Use this CLI command to exit from the EXEC mode.

Syntax

```
logout
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#logout

WS5100 release 3.0.0.0-200B
Login as 'cli' to access CLI.
WS5100 login:
```

4.1.21 mkdir

Priv Exec Command

Use this CLI command to create a new directory in the filesystem.

Syntax

```
mkdir DIR
```

Parameters

DIR	Directory name

Usage Guidelines

Example

```
WS5100#mkdir TestDIR
WS5100#
```

4.1.22 more

▶ *Priv Exec Command*

Use this CLI command to view the contents of a file.

Syntax

```
more FILE
```

Parameters

FILE	Displays the content of the file

Usage Guidelines

Example

```
WS5100#more flash:/log/messages.log
Sep 08 12:27:30 2006: %PM-5-PROCSTOP: Process

"radiusd" has been stopped
Sep 08 12:27:31 2006: %LICMGR-6-NEWLICENSE:

Licensed AP count changed to 48
Sep 08 12:27:31 2006: %CC-5-COUNTRYCODE:

config: setting country code to [in:
India]
Sep 08 12:27:31 2006: %DAEMON-6-INFO: radiusd

[460]: Ready to process requests.
Sep 08 12:27:35 2006: %DAEMON-6-INFO: init:

Starting pid 328, console
/dev/ttyS0
Sep 08 12:27:37 2006: %AUTH-6-INFO: login[328]:

root login  on `ttyS0' from
`Console'
Sep 08 12:27:47 2006: %IMI-5-USERAUTHSUCCESS:

User 'admin' logged in with role
of ' superuser' from auth source 'local'
Sep 08 12:28:01 2006: %NSM-6-DHCPDEFRT: Default

route with gateway
157.235.208.246 learnt via DHCP
Sep 08 12:28:01 2006: %NSM-6-DHCPIP: Interface
```

```
vlan1 acquired IP address
157.235.208.93/24 via DHCP
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11bg

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11a

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:12 2006: %MOB-6-MUADD: Station 00

-0F-3D-E9-A6-54: Added to
Mobility Database
Sep 08 12:29:12 2006: %CC-6-STATIONASSOC:

Station 00-0F-3D-E9-A6-54 associated
to radio 3 wlan 1
 -- MORE --, next page: Space, next line:

Enter, quit: Control-C
```

4.1.23 page

Priv Exec Command

Use this CLI command to toggle between the page.

Syntax

```
page
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#page
WS5100#
```

4.1.24 ping

Priv Exec Command

Use this CLI command to send ICMP echo messages.

Syntax

```
ping WORD
```

Parameters

WORD	Ping destination address or hostname.

Usage Guidelines

Example

```
WS5100#ping 157.235.208.39
PING 157.235.208.39 (157.235.208.39): 100 data bytes
128 bytes from 157.235.208.39: icmp_seq=0 ttl=64 time=2.3 ms
128 bytes from 157.235.208.39: icmp_seq=1 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=2 ttl=64 time=0.3 ms
128 bytes from 157.235.208.39: icmp_seq=3 ttl=64 time=0.2 ms
128 bytes from 157.235.208.39: icmp_seq=4 ttl=64 time=0.1 ms

--- 157.235.208.39 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.6/2.3 ms
WS5100#
```

4.1.25 pwd

Priv Exec Command

Use this CLI command to view the contents of the current directory.

Syntax

pwd

Parameters

None.

Usage Guidelines

Example

```
WS5100#pwd
flash:/
WS5100#
```

4.1.26 quit

Priv Exec Command

Use this CLI command to exit from the current mode and move down to previous mode.

Syntax

```
quit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#quit

WS5100 release 3.0.0.0-200B
Login as 'cli' to access CLI.
WS5100 login:
```

4.1.27 reload

Priv Exec Command

Use this CLI to halt the WS5100 Series Switch and perform a warm reboot.

Syntax

```
reload
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#reload
```

4.1.28 rename

Priv Exec Command

Use this CLI command to rename a file in the existing filesystem.

Syntax

```
rename FILE FILE
```

Parameters

FILE	FIle to be rename.

Usage Guidelines

Example

```
WS5100#rename flash:/TestDIR/ NewTestDir
WS5100#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006   cli_commands.save
  drwx   1024      Sat Sep  2 00:31:24 2006   NewTestDir

WS5100#
```

4.1.29 rmdir

▶ *Priv Exec Command*

Use this CLI command to delete a existing file from the file system.

Syntax

```
rmdir DIR
```

Parameters

DIR	Name of the Directory to be deleted.

Usage Guidelines

Example

```
WS5100#rmdir flash:/NewTestDir/
WS5100#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006
cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006   cli_commands.save
```

4.1.30 telnet

▶ *Priv Exec Command*

Use this command to open a telnet session.

Syntax

```
telnet WORD (PORT|)
```

Parameters

WORD	IP address or hostname of a remote system

Usage Guidelines

Example

```
WS5100#telnet 157.111.222.33

Entering character mode
Escape character is '^]'.

Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-6bigmem on an i686
login: cli
Password:
```

4.1.31 traceroute

Priv Exec Command

Use this CLI command to trace the route to destination.

Syntax

```
traceroute (WORD | ip WORD)
```

Parameters

WORD	Trace route to destination address or hostname
ip	IP Trace

Example

```
WS5100#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max, 38 byte
packets
 1  157.235.208.39 (157.235.208.39)  0.466 ms  0.363 ms  0.226 ms
WS5100#
```

4.1.32 upgrade

Priv Exec Command

Use this CLI command to upgrade the software image on the Ws5100 Series Switch.

Syntax

```
upgrade URL (background|)
```

Parameters

URL	Location of firmware image

Example

```
WS5100#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

update is /dev/hda6
Reading image file header
Removing other partition
Sep 08 15:57:18 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Making file system
Extracting files (this can take some time).Sep

08 15:57:23 2006: %KERN-6-INFO:
kjournald starting.  Commit interval 5 seconds.
Sep 08 15:57:23 2006: %KERN-6-INFO: EXT3 FS on

hda6, internal journal.
Sep 08 15:57:23 2006: %KERN-6-INFO: EXT3-fs:

mounted filesystem with ordered
data mode..
.......................
Sep 08 15:58:17 2006: %DIAG-4-CPULOAD: One

minute average load limit exceeded,
value is 100.00% limit is 99.90% (top process
kernel/ISR 100.00%)
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process
```

```
"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Version of firmware update file is 3.0.0.0-

19193X
Sep 08 15:58:44 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Creating LILO files
Running LILO
Successful
Sep 08 15:58:46 2006: %FWU-6-FWUDONE: Firmware

update successful, new version
is 3.0.0.0-19193X
WS5100#
```

4.1.33 upgrade-abort

▶ *Priv Exec Command*

Use this CLI command to abort the process of an ongoing upgrade.

Syntax

```
upgrade-abort
```

Parameters

None.

Usage Guidelines

Example

```
WS5100#upgrade-abort
% Error: No upgrade in progress

WS5100#upgrade tftp://157.235.208.105:/img

background
WS5100#Sep 08 16:01:38 2006: %KERN-4-WARNING:

EXT3-fs warning: maximal mount
count reached, running e2fsck is recommended.
Sep 08 16:01:38 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
%KERN-6-INFO: kjournald starting.  Commit

interval 5 seconds.
Sep 08 16:01:43 2006: %KERN-6-INFO: EXT3 FS on

hda6, internal journal.
Sep 08 16:01:43 2006: %KERN-6-INFO: EXT3-fs:

mounted filesystem with ordered
data mode..
WS5100#upgrade-abort
WS5100#
WS5100#show upgrade-status
Last Image Upgrade Status : Extracting files

(this can take some time).Aborted
Last Image Upgrade Time   : Fri Sep  8 16:01:54 2006
```

4.1.34 write

▶ *Priv Exec Command*

Use this command to write running configuration to memory or terminal

Syntax

```
write [memory | terminal]
```

Parameters

memory	Write to NV memory
terminal	Write to terminal

Usage Guidelines

Example

```
WS5100#write terminal
!
! configuration of WS5100 version 3.0.0.0-200B!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username manager privilege  superuser
!
!no country-code
logging console 7
no logging on
fallback enable
ftp password 1 810a25d76c31e495cc070bdf42e076f7c9b0a1cd
ip http server
ip http secure-trustpoint local
ip http secure-server
ip ssh
ip telnet
snmp-server manager v2
snmp-server manager v3
crypto isakmp identity address
crypto isakmp keepalive 10
crypto ipsec security-association lifetime kilobytes 4608000
!.....................................
```

5

Global Configuration Commands

The term **global** is used to indicate characteristics or features that affect the system as a whole. Global configuration mode is used to configure the system globally, or to enter specific configuration modes to configure specific elements such as interfaces or protocols. Use the *configure terminal* command, under PRIV EXEC, to enter global configuration mode.

The example below describes the process of entering global configuration mode from privileged EXEC mode:

```
WS5100# configure terminal
WS5100(config)#
```

NOTE The system prompt changes to indicate that you are now in global configuration mode. The prompt for global configuration mode consists of the host-name of the device followed by (config) and the pound sign (#).

Commands entered in global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved into the startup configuration file until you issue the *copy running-config startup-config* EXEC mode command.

5.1 Global Configuration Commands

Table 5.1 summarizes the Gloabl Config commands within the WS5100 Series Switch command line interface.

Table 5.1 Global Cnfiguration Command Summary

Command	Description	Ref.
aaa	Authentication, Authorization and Accounting.	page 5-4
access-list	Add an access list entry.	page 5-5
banner	Define a login banner.	page 5-6
boot	Reboots the wireless switch.	page 5-7
clrscr	the display screen.	page 2-3
country-code	Configure the country of operation. All existing radio configuration will be erased.	page 5-8
crypto	Encryption related commands.	page 5-11
do	Run commands from Exec mode.	page 5-16
end	End current mode and change to EXEC mode.	page 5-17
exit	End current mode and down to previous mode.	page 2-4
fallback	Configures software fallback feature.	page 5-18
ftp	Configure FTP Server.	page 5-19
help	Description of the interactive help system.	page 2-5
hostname	Set system's network name.	page 5-20
interface	Select an interface to configure.	page 5-21
ip	Internet Protocol (IP).	page 5-22

Command	Description	Ref.
license	license management command.	page 5-26
line	Configure a terminal line.	page 5-27
local	Local user authentication.	page 5-28
logging	Modify message logging facilities.	page 5-29
mac	Configure MAC access-lists.	page 5-31
no	Negate a command or set its defaults .	page 2-7
ntp	Configure NTP.	page 5-32
prompt	Set system's prompt.	page 5-36
radius-server	Enter radius-server mode.	page 5-37
redundancy	Configure redundancy group parameters.	page 5-39
service	Service Commands.	page 5-41
terminal	Show running system information.	page 2-19
snmp-server	Modify SNMP engine parameters.	page 5-43
terminal	Set terminal line parameters.	page 5-50
timezone	Configure the timezone.	page 5-51
username	Establish User Name Authentication.	page 5-52
vpn	vpn	page 5-53
wireless	Configure Wireless Parameters.	page 5-54

5.1.1 aaa

Global Configuration Commands

Displays the current aaa (Authentication,Authorization and Accounting) settings managed by WS5100 Series Wireless Switch.

Syntax

```
aaa (authentication(login(default(local|none|radius)))|nas|
vpn-authentication(primary(A.B.C.D))|secondary(A.B.C.D)))

aaa authentication login default {none|{local|radius}}
aaa nas WORD
aaa vpn-authentication (primary|secondary) A.B.C.D key  WORD (authport
PORT_RANGE |)
```

Parameters

authentication	Authentication configuration parameters
login	Set authentication lists for logins
default	The default authentication list
local	Use local user database
none	No authentication
radius	Use external radius server
nas	nas identifier. This parameter accepts a string of 64 charaters.
vpn-authentication	vpn authentication using radius
primary	primay address
secondary	secondary address
A.B.C.D	address

Usage Guidelines

Example

5.1.2 access-list

Global Configuration Commands

Use this CLI command to add an access list entry.

Syntax

```
access-list

access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(wlan <1-32>|)(log|) (rule-
precedence <1-500>|)

access-list (<100-199>|<2000-2699>) (deny|permit|mark (8021p <0-7> | tos
<0-255>)) (icmp) (A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M | host A.B.C.D
| any)(<0-255> | <0-255> <0-255> |)(wlan <1-32>|)(log|) (rule-precedence
<1-500> |)

access-list (<100-199>|<2000-2699>) (deny|permit|mark (8021p <0-7> | tos
<0-255>)) (ip) (A.B.C.D/M | host A.B.C.D | any)(A.B.C.D/M | host A.B.C.D |
any)(wlan <1-32>|)(log|) (rule-precedence <1-500> |)

access-list (<100-199>|<2000-2699>) (deny|permit|mark (8021p <0-7> | tos
<0-255>)) (tcp|udp) (A.B.C.D/M | host A.B.C.D | any)(eq <1-65535> | range
<1-65535> <1-65535> |)(A.B.C.D/M | host A.B.C.D | any)(eq <1-65535> |
range <1-65535> <1-65535> |)(wlan <1-32>|)(log|) (rule-precedence <1-500>
|)
```

Parameters

	Enter a brief description

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

5.1.3 banner

Global Configuration Commands

Use this CLI command to define a login banner for the WS5100 Series Wireless Switch.

Syntax

```
banner(motd(LINE|default))
```

Parameters

motd	Set Message of the Day banner
LINE	Custom MOTD string
default	Default MOTD string

Usage Guidelines

Example

```
WS5100(config)#banner motd Welcome to my WS5100 CLI
WS5100(config)


WS5100 release 3.0.0.0-200B
Login as 'cli' to access CLI.
WS5100 login: cli
Welcome to my WS5100 CLI
Welcome to my WS5100 CLI
WS5100>

WS5100(config)#banner motd default
WS5100(config)#

WS5100 release 3.0.0.0-200B
Login as 'cli' to access CLI.
WS5100 login: cli
Welcome to CLI
Welcome to CLI

WS5100>
```

5.1.4 boot

Global Configuration Commands

This CLI command is used to reboot the WS5100 Series Wireless Switch.

Syntax

```
boot(system [primary|secondary])
```

Parameters

system	Specify boot image to use after reboot
primary	Primary image
secondary	Secondary image

Usage Guidelines

Example

```
WS5100(config)#boot system primary
Wireless switch will be rebooted, do you want to continue? (y/n):y
Do you want to save teh configuration? (y/n):y

The system is going down NOW !!

% Connection is closed by administrator!
Please stand by while rebooting the system.
```

5.1.5 country-code

Global Configuration Commands

Use this CLI command to configure the country of operation.

Syntax

```
country-code
```

Parameters

None.

Usage Guidelines

All existing radio configuration will be erased when this command is used.

Example

```
WS5100(config)#country-code ?
  ae  United Arab Emirates
  ar  Argentina
  at  Austria
  au  Australia
  ba  Bosnia Herzegovina
  be  Belgium
  bg  Bulgaria
  bh  Bahrain
  bm  Bermuda
  br  Brazil
  bs  Bahamas
  by  Belarus
  ca  Canada
  ch  Switzerland
  cl  Chile
  cn  China
  co  Colombia
  cr  Costa Rica
  cy  Cyprus
  cz  Czech Republic
  de  Germany
  dk  Denmark
  do  Dominican Republic
  ec  Ecuador
  ee  Estonia
  eg  Egypt
  es  Spain
  fi  Finland
  fr  France
  gb  United Kingdom
```

```
gr  Greece
gt  Guatemala
gu  Guam
hk  Hong Kong
hn  Honduras
hr  Croatia
ht  Haiti
hu  Hungary
id  Indonesia
ie  Ireland
il  Israel
in  India
is  Iceland
it  Italy
jo  Jordan
jp  Japan
kr  South Korea
kw  Kuwait
kz  Kazakhstan
li  Liechtenstein
lk  Sri Lanka
lt  Lithuania
lu  Luxembourg
lv  Latvia
ma  Morocco
mt  Malta
mx  Mexico
my  Malaysia
nl  Netherlands
no  Norway
nz  New Zealand
om  Oman
pe  Peru
ph  Philippines
pk  Pakistan
pl  Poland
pt  Portugal
qa  Qatar
ro  Romania
ru  Russia
sa  Saudi Arabia
se  Sweden
sg  Singapore
si  Slovenia
sk  Slovak Republic
th  Thailand
tr  Turkey
tw  Taiwan
ua  Ukraine
```

```
  us  United States
  uy  Uruguay
  ve  Venezuela
  vn  Vietnam
  za  South Africa
WS5100(config)#country-code
```

5.1.6 crypto

Global Configuration Commands

Use this CLI commands to configure the encryption related commands.

NOTE `crypto isakmp(`*`policy`*`)`**`Priority`** leads you to `config-crypto-isakmp` instance. For more details see *crypto-isakmp on page 6-1*.

`crypto isakmp(`*`client`*`)`**`configuration group default`** leads you to `config-crypto-group` instance. For more details see *crypto-group on page 7-1*.

`crypto isakmp(`*`peer`*`)`**`IP Address`** leads you to `config-crypto-peer` instance. For more details see *crypto-peer on page 8-1*.

`crypto ipsec` **`transformset`** `(name) <value>` leads you to config-`crypto-ipsec.` Use the crypto ipsec transform-set command to define the transform configuration for securing data (e.g., esp-3des, esp-sha-hmac, etc.). The transform-set is then assigned to a crypto map using the map's set transform-set command. For more details see *crypto-ipsec on page 9-1*

`crypto pki trustpoint` mode leads to `(config-trustpoint)` instance. For more details see *crypto-trustpoint Instance on page 11-1*.

Syntax

```
crypto(ipsec|isakmp|key|map|pki)

crypto ipsec(security-association|transform-set)
crypto ipsec security-association lifetime(kilobyte|Seconds)WORD
crypto ipsec transform-set(ah-md5-hmac|ah-sha-hmac|esp-3des|esp-aes|
esp-aes-192|esp-aes-256|esp-des|esp-md5-hmac|esp-sha-hmac)

crypto isakmp(client|identity|keepalive|key|peer|policy)
crypto isakmp client (configuration)(group)(default)
crypto isakmp(identity|keepalive|key|peer|policy)

crypto key(export|generate|import|zeroize)
crypto key (export|import)rsa<indentifier>(tftp|ftp)
crypto key generate(rsa <indentifier>)<key pair> <key pair>
crypto zeroize (rsa <identifier>)
```

```
crypto map (map name)<sequence number> (isakmp|manual)dynamic

crypto pki(authenticate|enroll|export|import|trustpoint)
crypto pki authenticate <name> (terminal|tftp|ftp)
crypto pki enroll<name> (request|self-signed)
crypto pki export <name> (request|trustpoint)(tftp|ftp)
```

Parameters

ipsec	ipsec configuration
security association	security association
lifetime(kilobytes|seconds) *<value>*	IPSec S-A lifetime. • kilobytes – lifetime in kilobytes • seconds – lifetime in seconds
transform-set *<setname1>....<setname 9>*	Use the crypto ipsec transform-set command to define the transform configuration for securing data. • ah-md5-hmac • ah-sha-hmac • esp-3des • esp-aes • esp-aes-192 • esp-aes-256 • esp-des • esp-md5-hmac • esp-sha-hmac The transform-set is then assigned to a crypto map using the map's set transform-set command. See *crypto-ipsec on page 9-1*.
isakmp	Internet Security Association and Key Management Protocol.
client	`crypto isakmp(client)configuration group default` leads you to `config-crypto-group` instance. For more details see *crypto-group on page 7-1*.
identity	Global Identity type
keepalive	Number of seconds between DPD messages

key	peer key
peer	remote peer
policy	Isakmp Policy
key	Authentication key management
export | import	
`rsa<indentifier>`	Rsa Keypair identifier Associated with Keypair
`(tftp|ftp)`	URL to send the key to.
generate	
`<key pair>`	Size of Keypair. Shoule be between *1024-2048*
zeroize	
map<name>	crypto map entry name of 32 character length
isakmp	Ipsec-isakmp
manual	Ipsec-manual
dynamic	dynamic map entry (remote VPN configuration)
pki	Configure certificate parameters.Public Key Infrastructure is a protocol that creates encrypted public keys using digital certificates from Certificate Authorities. PKI ensures that each online party is who they claim to be.
authenticate	Authenticate and import CA Certificate
enroll	Enroll
export	Export
import	Import
trustpoint	Define a CA trustpoint
request	Certificate Request mode of enrollment
self-signed	Selfsigned Mode of enrollment

trustpoint	Trustpoint Configuration
terminal	Copy & Paste mode of enrollment

Usage Guidelines

Currently a peer address can be deleted with wrong isakmp value. Crypto currently matches only the IP address when a **no** command is issued. This feature will be corrected in the next release.

```
WS5100(config)#crypto isakmp key 12345678 address 4.4.4.4

WS5100(config)#show running-config
configuration of WS5100 version 3.0.0.0-200B!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
.....................................
.............................
crypto isakmp key 12345678 address 4.4.4.4
crypto ipsec security-association lifetime kilobytes 4608000
WS5100(config)#

WS5100(config)#no crypto isakmp key 12348 address 4.4.4.4
WS5100(config)#
```

In the example above, **key 12345678** is associated with IP **address 4.4.4.4**. Currently you can delete this key by using the no command and a wrong key number.

Example

```
WS5100(config)#crypto pki ?
```

```
  authenticate  Authenticate and import CA Certificate
  enroll        Enroll
  export        Export
  import        Import
  trustpoint    Define a CA trustpoint

WS5100(config)#crypto pki trustpoint ?
  WORD  Trustpoint Name

WS5100(config)#crypto pki trustpoint Test
WS5100(config-trustpoint)#?
Trustpoint Config commands:
  clrscr        Clears the display screen
  company-name  Company Name(Applicable only for request)
  email         email
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  fqdn          Domain Name Configuration
  help          Description of the interactive help system
  ip-address    Internet Protocol (IP)
  no            Negate a command or set its defaults
  password      Challenge Password(Applicable only for request)
  rsakeypair    Rsa Keypair to associate with the trustpoint
  service       Service Commands
  show          Show running system information
  subject-name  Subject Name is a collection of required parameters to
                configure a trustpoint.

WS5100(config-trustpoint)#
```

5.1.7 do

Global Configuration Commands

Use this CLI command to run commands from the other exec mode — User Exec and Priv Exec modes.

Syntax

```
do (command of other mode)
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config)#do ping 157.235.208.69
PING 157.235.208.69 (157.235.208.69): 100 data bytes
128 bytes from 157.235.208.69: icmp_seq=0 ttl=64 time=0.1 ms
128 bytes from 157.235.208.69: icmp_seq=1 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=2 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=3 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=4 ttl=64 time=0.0 ms

--- 157.235.208.69 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
WS5100(config)#
```

NOTE In the example above, `ping` is a PRIV EXEC command.

5.1.8 end

Global Configuration Commands

Use this CLI command to end the current mode and change to Exec mode

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config)#end

WS5100#?
Priv Exec commands:
  acknowledge    Acknowledge alarms
  archive        Manage archive files
  autoinstall    autoinstall configuration command
  cd             Change current directory
  ........................................
  ........................................
```

5.1.9 fallback

Global Configuration Commands

Use this CLI command to enable and configures software fallback feature. Failure to boot with configured "use on boot" image allows booting with other image.

Syntax

```
fallback(enable)
```

Parameters

enable	Enable software fallback feature.

Usage Guidelines

Example

```
WS5100(config)#fallback  enable
WS5100(config)#
```

5.1.10 ftp

Global Configuration Commands

Use this CLI command to configure the FTP server.

Syntax

```
ftpenable
ftp password(0|1|LINE)
ftp rootdir(DIR)
```

Parameters

enable	Enable FTP Server.
password	Configure FTP password. You can set the password using one of the folllowing options: • 0 — Password is specified UNENCRYPTED. • 1 — Password is encrypted with SHA1 algorithm. • LINE — Password.
rootdir	Configure FTP root dir. Set the ROOT directory location of the FTP server using: • DIR — Used to set root dir of the ftp server.

Usage Guidelines

Example

```
WS5100(config)#ftp enable
WS5100(config)#
```

5.1.11 hostname

Global Configuration Commands

Use this CLI command to change the name of the systems network.

Syntax

```
hostname(WORD)
```

Parameters

WORD	USed to provide the name for the systems network.

Usage Guidelines

Example

```
WS5100(config)#hostname Eldorado
Eldorado(config)#
```

5.1.12 interface

Global Configuration Commands

Use this CLI command to select and interface to confiugre.

NOTE interface mode leads to `config-if` instance. For more details see *interface Instance on page 12-1*.
The prompt changes from `ws5100(config) #` to `ws5100(config-if)`

Syntax

```
interface(IFNAME|eth|tunnel|vlan)
```

Parameters

IFNAME	Interface name
eth	Ethernet interface
tunnel	Tunnel interface
vlan	Vlan interface

Usage Guidelines

Example

```
WS5100(config)#interface eth 2
WS5100(config-if)#

WS5100(config)#interface vlan 2
WS5100(config-if)#
```

5.1.13 ip

Global Configuration Commands

NOTE Using `access-list extended` command leads you to **`(config-ext-nacl)`** instance. For more details see *Extended ACL Instance on page 13-1*

Using `access-list extended` command leads you to **`(config-std-nacl)`** instance. For more details see *Standard ACL Instance on page 14-1*

Syntax

```
ip(access-list|default-gateway|dhcp|domain-lookup|domain-
name|http|local|name-server|nat|route|routing|ssh|telnet)

ip(access-list(extended(<100-199|<2000-2699>|WORD)|standard(<1-99>|<1300-
1999>|WORD))

ip default-gateway(A.B.C.D)

ip dhcp(bootp|excluded-address|option|ping|pool|restart)
ip dhcp bootp(ignore)
ip dhcp excluded-address(A.B.C.D)
ip dhcp option(option name)
ip dhcp ping(timeout(<1-10>))
ip dhcp pool(pool name)
ip dhcp restart

ip domain-lookup

ip domain-name(WORD)

ip http(secure-server|secure-trustpoint(WORD)|server(localhost))

ip local(pool(default(low-ip-address(A.B.C.D))))

#ip name-server(A.B.C.D)

ip nat(inside|outside)
ip nat(inside(destination|source))
ip nat(inside(destination(static(A.B.C.D))|source))
ip nat(inside(destination|source(list(WORD)|static(A.B.C.D))
ip nat(outside(destination|source))
```

```
ip nat(outside(destination(static(A.B.C.D))|source))
ip nat(outside(destination|source(list(WORD)|static(A.B.C.D))

ip route(A.B.C.D|A.B.C.D/M)

ip routing

ip ssh(port|rsa)
ip ssh(port(<0-65536>))
ip ssh(rsa(keypair-name(WORD)))

ip telnet(port(<0-65535>))
```

Parameters

access-list	ACL Config. Using the access list parameter options you enter the **`ext-nacl`** context and **`std-nacl`** context. The prompt now changes to the context you have entered. For more details,see *Extended ACL Instance on page 13-1* for extended ACL and *Standard ACL Instance on page 14-1* for standard ACL.
default-gateway	Configure default gateway
A.B.C.D	IP gateway address
dhcp	DHCP Server configuration
bootp	BOOTP specific configuration
ignore	Configure DHCP Server to ignore BOOTP requests
excluded-address	Prevent DHCP Server from assigning certain addresses
A.B.C.D	Low IP Address
option	Define DHCP server option name.
ping	Specify ping parameters used by DHCP Server
timeout	Specify ping timeout between 1-10 seconds.
pool	Configure DHCP server address pool
restart	Restart DHCP Server to get the DHCP config changes into effect
domain-lookup	Enable Domain Name Service (DNS)

domain-name	Set default domain for DNS
http	Hyper Text Transfer Protocol (HTTP)
secure-server	Secure HTTP server (HTTPS)
secure-trustpoint	Enter the name of the trustpoint to be used for secure connection
server	HTTP server
localhost	Used only to serve requests from localhost
local	vpn local ip pool configuration
pool	Address pool
default	
low-ip-address	
A.B.C.D	Internet Protocol
name-server	Add a Nameserver to the DNS
A.B.C.D	IP address of Nameserver to add
nat	Network Address Translation (NAT)
(inside|outside)	
destination	Destination address
static	Static
A.B.C.D	Inside local IP address (A.B.C.D)
source	Source address
list	Access list
WORD	Access list name
static	
A.B.C.D	Inside local IP address (A.B.C.D)
route	Establish static routes

A.B.C.D	IP destination prefix
A.B.C.D/M	IP destination prefix
routing	Turn on IP routing
ssh	Secured SHell (SSH) server
port	Listening port. Value can be anything between 0-65536.
rsa	RSA encryption key
keypair-name	Configure RSA keypair to be used for encryption
WORD	RSA keypair name
telnet	Telnet server
port	Value of the listening port. The value can be anything between 0-65535

Usage Guidelines

By using the `ip access-list` parameter you enter the following contexts:

- ext-nacl — extended ACL. For more details see *Extended ACL Instance on page 13-1*.
- std-nacl — Standard ACL. For more details see *Standard ACL Instance on page 14-1*.
- You can clear the ip dhcp binding using the *clear* command.

NOTE To delete Standard/Extended and MAC ACL use **`no access-list <access-list name>`** under the Global Config mode.

Example

```
WS5100(config)#ip access-list extended TestACL
WS5100(config-ext-nacl)#

WS5100(config)#ip access-list standard TestStdACL
WS5100(config-std-nacl)#
```

5.1.14 license

Global Configuration Commands

<<< Text here>>>

Syntax

```
license
```

Parameters

WORD	Enter the name of the feature for which you wish to add license.

Usage Guidelines

Example

5.1.15 line

Global Configuration Commands

Use this CLI command to configure the terminal line.

Syntax

```
line(console|vty)
```

Parameters

console	Primary terminal line.You can configure a value between 0-0.
vty	Virtual terminal.You can configure a value between 0-871.

Usage Guidelines

Example

5.1.16 local

Global Configuration Commands

Use this CLI command to set the username and password for local user authentication.

Syntax

```
local(username,password)
```

Parameters

username	Enter local user name. The username can be a string of upto 64 characters.
password	Enter local user password. The password can be a string of upto 21 characters.

Usage Guidelines

Example

```
WS5100(config)#local username "Noble Man" password "Noble Soul"
```

5.1.17 logging

Global Configuration Commands

Use this CLI command to modify message logging facilities of the WS5100 Series Wireless Switch.

Syntax

```
logging(aggregation-time|buffered|console|facility|host|monitor|on|syslog)

logging aggregation-time(<1-20>)

logging buffered(<0-7>|alerts|critical|debugging|emergencies|errors|
informational|notifications|warnings)
```

Parameters

aggregation-time	Set number of seconds for aggregating repeated messages. The value can be configured between 1-60 seconds.
buffered	Set buffered logging level.
console	Set console logging level.
monitor	Set terminal lines logging level.
syslog	Set syslog servers logging level.
<0-7>	Enter the Logging severity level.Can be between 0-7.
alerts	Immediate action needed, (severity=1).
critical	Critical conditions, (severity=2).
debugging	Debugging messages, (severity=7).
emergencies	System is unusable, (severity=0).
errors	Error conditions, (severity=3).
informational	Informational messages, (severity=6).
notifications	Normal but significant conditions, (severity=5).
warnings	Warning conditions, (severity=4).
facility	Syslog facility in which log messages are sent.
local0	Syslog facility local0

local1	Syslog facility local1
local2	Syslog facility local2
local3	Syslog facility local3
local4	Syslog facility local4
local5	Syslog facility local5
local6	Syslog facility local6
local7	Syslog facility local7
host	Configure remote host to receive log messages.
A.B.C.D	Remote host's IP address
on	Enable logging of system messages.

Usage Guidelines

Example

```
WS5100(config)#logging aggregation-time 20
WS5100(config)#
```

5.1.18 mac

Global Configuration Commands

Use this CLI command to configure MAC access-lists.

Syntax

```
mac(access-list(extended(WORD)))
```

Parameters

access-list	ACL config for the MAC address.
extended	MAC Extended ACL
WORD	Enter the name of the ACL.

Usage Guidelines

To delete Standard/Extended and MAC ACL use **`no access-list <access-list name>`** under the Global Config mode.

Example

```
WS5100(config)#mac access-list extended Test1
WS5100(config-ext-macl)#
```

NOTE By using the `ip access-list` parameter you enter the following contexts:

- .ext-macl — extended MAC ACL. For more details see .Extended MAC ACL Instance on page 15-1

5.1.19 ntp

Global Configuration Commands

Use this CLI command to configure NTP over the WS5100 Series Wireless Switch.

Syntax

```
ntp(access-group|authenticate|authentication-key|autokey|
broadcast|broadcastdelay|master|peer|server|trusted-key)

ntp access-group(peer|query-only|serve|serve-only)
ntp access-group peer(<1-99>|<1300-1999>)
ntp access-group query-only(<1-99>|<1300-1999>)
ntp access-group serve(<1-99>|<1300-1999>)
ntp access-group serve-only(<1-99>|<1300-1999>)

ntp authenticate

ntp authentication-key(md5(WORD))

ntp autokey(client-only|host)

ntp broadcast(client|destination)
ntp broadcast destination(WORD(key|version))
ntp broadcast destination WORD key <1-65534>
ntp broadcast destination WORD version <1-4>

ntp broadcastdelay <1-999999>

ntp master <1-15>

ntp peer(WORD)
ntp peer WORD(autokey|key|prefer|version)
ntp peer WORD autokey(prefer|version<1-4>)
ntp peer WORD key(<1-65534>(prefer|version(<1-4>)))
ntp peer WORD prefer (version<1-4>)
ntp peer TestPeer version<1-4>

ntp server(WORD)
ntp server WORD(autokey|key|prefer|version)
ntp server WORD autokey(prefer|version<1-4>)
ntp server WORD key(<1-65534>(prefer|version(<1-4>)))
ntp server WORD prefer (version<1-4>)
ntp server TestPeer version<1-4>

ntp trusted-key <1-65534>
```

Parameters

access-group	Control NTP access
peer	Provide full access
query-only	Allow only control queries
serve	Provide server and query access
serve-only	Provide only server access
<1-99>	Standard IP access list
<1300-1999>	Standard IP access list (expanded range)
authenticate	Authenticate time sources
authentication-key	Authentication key for trusted time sources
md5	MD5 authentication
WORD	Authentication key
autokey	Enable NTP autokey authentication scheme
client-only	Switch will be a client to other trusted-hosts in the autokey group
host	Configure the switch as a trusted host
broadcast	Configure NTP broadcast service
client	Listen to NTP broadcasts
destination	Configure broadcast destination address
WORD	Destination broadcast IP address
key	Broadcast key
<1-65534>	Key ID
version	NTP version
<1-4>	NTP Version number
broadcastdelay	Estimated round-trip delay
<1-999999>	Round-trip delay in microseconds

master	Act as a NTP master clock
<1-15>	Stratum number for the NTP master clock
peer	Configure NTP peer
server	Configure NTP server
WORD	
autokey	Configure autokey peer authentication scheme
key	Configure peer authentication key
<1-65534>	Peer key number
prefer	Prefer this peer when possible
version	Configure NTP version
<1-4>	NTP version number
trusted-key	Key numbers for trusted time sources
<1-65534>	Key number

Usage Guidelines

Example

```
WS5100(config)#ntp peer ?
  WORD  Name/IP address of peer

WS5100(config)#ntp peer TestPeer ?
  autokey  Configure autokey peer authentication scheme
  key      Configure peer authentication key
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer autokey ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer autokey prefer ?
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer autokey prefer version ?
  <1-4>  NTP version number

WS5100(config)#ntp peer TestPeer autokey prefer version 3
WS5100(config)#

WS5100(config)#ntp peer TestPeer key ?
  <1-65534>  Peer key number

WS5100(config)#ntp peer TestPeer key 20 ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer key 20 prefer ?
  version  Configure NTP version
  <cr>

WS5100(config)#ntp peer TestPeer key 20 prefer version ?
  <1-4>  NTP version number

WS5100(config)#ntp peer TestPeer key 20 prefer version 2
Invalid server name "TestPeer" provided. Please enter a valid name
WS5100(config)#
```

5.1.20 prompt

Global Configuration Commands

Use this CLI command to configure and set the systems prompt.

Syntax

```
prompt(LINE)
```

Parameters

LIMNE	Enter the new prompt that will be displayed by the system/WS5100 Series Wireless Switch.

Usage Guidelines

Example

```
WS5100(config)#prompt NobleMan
NobleMan
```

5.1.21 radius-server

Global Configuration Commands

Use this CLI command to enter the RADIUS Server mode. The WS5100 system prompt will change from the default config mode to Radius server mode.

NOTE `radius-server local` mode leads you to the radius-server context. For more details see *Radius Server Instance on page 16-1*

Syntax

```
radius-server(host|key|local|retransmit|timeout)
radius-server host (A.B.C.D)
radius-server key(0|2| LINE)
radius-server local
radius-server retransmit <0-100>
radius-server timeout<1-1000>
```

Parameters

host	Specify a RADIUS server
A.B.C.D	IP address of RADIUS server
key	Encryption key shared with the radius servers
0	Password is specified UNENCRYPTED
2	Password is encrypted with password-encryption secret
LINE	Text of shared key, upto 127 characters
local	Configure local radius server parameters.This takes you to a new **config-radius-server** context. Refer *Radius Server Instance* for more details.
retransmit	Specify the number of retries to active server
<0-100>	Number of retries for a transaction (default is 3)
timeout	Time to wait for a RADIUS server to reply
<1-1000>	Wait time (default 5 seconds)

Usage Guidelines

Example

```
WS5100(config)#radius-server local
WS5100(config-radsrv)#
```

5.1.22 redundancy

Global Configuration Commands

Use this CLI command to configure redundancy group parameters.

Syntax

```
redundancy(discovery-period|enable|group-id|handle-stp|
heartbeat-period|hold-period|interface-ip|member-ip|mode)

redundancy discovery-period <10-60>
redundancy enable
redundancy group-id <1-65535>
redundancy handle-stp(enable)
redundancy heartbeat-period
redundancy hold-period <10-255>
redundancy interface-ip(A.B.C.D)
redundancy member-ip (A.B.C.D)
redundancy mode(primary|standby)
```

Parameters

discovery-period	Set the redundancy discovery interval.
<10-60>	discovery time in secs (default is 30)
enable	Enable redundancy protocol.
group-id	Set the redundancy group id
<1-65535>	Redundancy group Id
handle-stp	Delay the redundancy protocol state machine exec, considering STP.
enable	Set handle-stp to true
heartbeat-period	Set the redundancy heartbeat interval.The `heartbeat-period` must always be less than the `hold-period.`
<1-255>	heartbeat interval in secs (default is 5)
hold-period	Set the redundancy hold interval.
<10-255>	hold interval in secs (default is 15)
interface-ip	Set redundancy interface IP address.
A.B.C.D	IP address of the switch

member-ip	Add member to this redundancy group.
A.B.C.D	IP address of the member
mode	set the redundancy mode.
primary	mode can be primary
standby	mode can be standby

Usage Guidelines

Example

```
WS5100(config)#redundancy discovery-period 20
WS5100(config)#

WS5100(config)#redundancy handle-stp enable
WS5100(config)#

WS5100(config)#redundancy heartbeat-period 20
WS5100(config)#

WS5100(config)#redundancy hold-period 25
WS5100(config)#

WS5100(config)#redundancy mode primary
WS5100(config)#
```

5.1.23 service

Global Configuration Commands

Use this CLI commands to retrive system data that includes tables, log files, configuration, status and operation, for use in debugging and problem resolution while troubleshooting the WS5100 Series Wireless Switch configuration.

Syntax

```
service(advanced-vty|ap|clear|dhcp|diag-shell|password-
encryption|pm|prompt|radius|save-cli|set|show|start-shell|terminal-
length|tethereal|wireless)
```

Parameters

advanced-vty	Enable advanced mode vty interface
ap	access-port serviceability parameters
clear	Remove specified support information
dhcp	Enable the DHCP Server service
diag-shell	Provide diag shell access
password-encryption	Encrypt passwords in configuration
pm(max-sys-restarts| sys-restart)	Process Monitor. • max-sys-restarts – Maximum number of times PM will restart the system because of a failed processes • sys-restart – Enable PM to restart the system when a processes fails **NOTE** The process restart is one count lesser than what is configured.
prompt	Enable crash-info prompt
radius	Enable radius server
save-cli	Save CLI tree for all modes in html format
set	Set service parameters
show	Show running system information

start-shell	Provide shell access
terminal-length	System wide terminal length configuration
tethereal	Dump and analyze network traffic
wireless	Wireless parameters

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

5.1.24 snmp-server

Global Configuration Commands

USe this CLI command to modify SNMP engine parameters.

Syntax

```
snmp-server(community|contact|enable|host|location|manager|sysname|user)
snmp-server community(WORD(ro|rw))
snmp-server contact LINE
snmp-server enable traps
     (all|miscellaneous|nsm|redundancy|snmp|wireless|wireless-statistics)

snmp-server enable traps all

snmp-server enable traps miscellaneous
(lowFsSpace|processMaxRestartsReached|savedConfigModified)

snmp-server enable traps nsm dhcpIPChanged

snmp-server enable traps redundancy
(adoptionExceeded|grpAuthLevelChanged|memberDown|memberMisConfigured|
 memberUp)

snmp-server enable traps snmp
(authenticationFail|coldstart|linkdown|linkup)

snmp-server enable traps wireless (ap-detection|ids|radio|
self-healing|station)
snmp-server enable traps wireless  ap-detection externalAPDetected
snmp-server enable traps wireless  ids
(excessiveAuthAssociation|excessiveProbes)
snmp-server enable traps wireless radio(adopted|detectedRadar|unadopted)
snmp-server enable traps wireless self-healing activated
snmp-server enable traps wireless station
(associated|deniedAssociationAsPortCapacityReached|
deniedAssociationOnCapability|deniedAssociationOnErr|
deniedAssociationOnInvalidWPAWPA2IE|deniedAssociationOnRates|
deniedAssociationOnSSID|deniedAssociationOnShortPream|
deniedAssociationOnSpectrum|deniedAuthentication|disassociated|
radiusAuthFailed|tkipCounterMeasures)

snmp-server enable traps wireless-statistics
(min-packets|mobile-unit|radio|wireless-switch|wlan)
snmp-server enable traps wireless-statistics min-packets <1-65535>
snmp-server enable traps wireless-statistics mobile-unit
(avg-bit-speed-less-than|avg-retry-greater-than|avg-signal-less-than|
gave-up-percent-greater-than|nu-percent-greater-than|
pktsps-greater-than|tput-greater-than|undecrypt-percent-greater-than)
```

```
snmp-server enable traps wireless-statistics radio
(avg-bit-speed-less-than|avg-retry-greater-than|avg-signal-less-than|
gave-up-percent-greater-than|nu-percent-greater-than|
num-mobile-units-greater-than|pktsps-greater-than|tput-greater-than|
undecrypt-percent-greater-than)
snmp-server enable traps wireless-statistics wireless-switch
(num-mobile-units-greater-than|pktsps-greater-than|tput-greater-than)

snmp-server enable traps wireless-statistics wlan
(avg-bit-speed-less-than|avg-retry-greater-than|avg-signal-less-than|
gave-up-percent-greater-than|nu-percent-greater-than|
num-mobile-units-greater-than|pktsps-greater-than|tput-greater-than|
undecrypt-percent-greater-than)

snmp-server host(A.B.C.D)
snmp-server location (LINE)
snmp-server manager(all|v2|v3)
snmp-server sysname

snmp-server user(manager|operator)
snmp-server user manager v3(auth|encrypted)
snmp-server user manager v3 (auth|encrypted) md5 PASSWD
```

Parameters

(community)	Set community string and access privileges
ro	Read-only access with this community string
rw	Read-write access with this community string
(contact)	Text for mib object sysContact
LINE	Identification of the contact person for this managed node
(enable) traps ( )	Enable SNMP traps
all	enable all traps
miscellaneous ( )	Enable miscellaneous traps
lowFsSpace	Available file system space is lower than the limit
processMaxRestartsReached	Process has reached max restart
savedConfigModified	Saved configuration has been modified
nsm	Enable nsm traps
dhcpIPChanged	DHCP IP changed

redundancy ( )	Enable redundancy traps
adoptionExceeded	Redundancy port adoption exceeded
grpAuthLevelChanged	Redundancy group Authorization Level changed
memberDown	Redundancy member down
memberMisConfigured	Redundancy member mis-configuration
memberUp	Redundancy member up
snmp ( )	Enable SNMP traps
authenticationFail	Enable authentication failure trap
coldstart	Enable coldStart trap
linkdown	Enable linkDown trap
linkup	Enable linkUp trap
wireless ( )	Enable wireless traps
ap-detection ( )	Enable wireless AP detection traps
externalAPDetected	External AP detected
ids ( )	Enable wireless IDS traps
excessiveAuthAssociation	Excessive association authentication
excessiveProbes	Excessive probes
radio ( )	Enable wireless radio traps
adopted	Radio adopted
detectedRadar	Radio detected radar
unadopted	Radio unadopted
self-healing ( )	Enable self healing traps
activated	Self healing activated
station ( )	Enable wireless station traps

associated	Wireless station associated
deniedAssociationAsPort CapacityReached	Wireless station denied association due to port capacity reached
deniedAssociationOnCapability	Wireless station denied association due to unsupported capability
deniedAssociationOnErr	Wireless station denied association due to internal error
deniedAssociationOnInvalid WPAWPA2IE	Wireless station denied association due to invalid/absent WPA/ WPA2 IE
deniedAssociationOnRates	Wireless station denied association due to incompatible Transmission rates
deniedAssociationOnSSID	Wireless station denied association due to invalid SSID
deniedAssociationOnShort Pream	Wireless station denied association due to lack of short preamble support
deniedAssociationOnSpectrum	Wireless station denied association due to lack of spectrum management capability
deniedAuthentication	Wireless station denied 802.11 authentication
disassociated	Wireless station disassociated
radiusAuthFailed	Wireless station failed radius authentication
tkipCounterMeasures	TKIP counter measures invoked
wireless-statistics ( )	Modify wireless-stats rate traps
min-packets	Minimum packets for sending the trap. This can be set with a decimal number in the range of <1-65535>
mobile-unit ( )	Modify mobile-unit rate traps
radio ( )	Modify radio rate traps
wireless-switch ( )	Modify wireless-switch rate traps
wlan ( )	Modify wlan rate traps

avg-bit-speed-less-than < >	Average bit speed in Mbps is less than — < A decimal number greater than 0.00 and less than or equal to 54.00>
avg-retry-greater-than < >	Average retry is greater than — < A decimal number greater than 0.00 and less than or equal to 16.00>
avg-signal-less-than < >	Average signal in dBm is less than — <A decimal number less than -0.00 and greater than or equal to -120.00>
gave-up-percent-greater-than < >	percentage of pkts dropped is greater than — <A decimal number greater than 0.00 and less than or equal to 100.00>
nu-percent-greater-than < >	percentage of non-unicast pkts is greater than — <A decimal number greater than 0.00 and less than or equal to 100.00>
pktsps-greater-than < >	Packets per sec is greather than — < A decimal number greater than 0.00 and less than or equal to 100000.00>
tput-greater-than < >	Throughput in Mbps is greather than — <A decimal number greater than 0.00 and less than or equal to 100000.00>
undecrypt-percent-greater-than < >	percentage of undecryptable pkts is geater than — <A decimal number greater than 0.00 and less than or equal to 100.00>
num-mobile-units-greater-than < >	Number of associated mobile-unit is greater than a decimal number in the range of <1-4096>
host	snmp server host
A.B.C.D	snmp server host IP-address
location	Text for mib object sysLocation
manager	Enable SNMP manager
all	Enable SNMP version v2 and v3
v2	Enable SNMP version v2
v3	Enable SNMP version v3
sysname	snmp system name
user	Define a user who can access SNMP engine
manager	Manager user

operator	Operator user
v3 ( )	User using v3 security model
auth ( )	Authentication parameters for the user
encrypted ( )	Specifying password as md5 digests
md5	Use HMAC MD5 algorithm for authentication
PASSWD	Authentication password for user

Usage Guidelines

Example

```
WS5100(config)#snmp-server community TestCommunity ro
WS5100(config)#

WS5100(config)#snmp-server contact TestManager
WS5100(config)#

WS5100(config)#snmp-server enable traps all
WS5100(config)#

WS5100(config)#snmp-server enable traps miscellaneous lowFsSpace
WS5100(config)#


WS5100(config)#snmp-server enable traps redundancy memberUp
WS5100(config)#

WS5100(config)#snmp-server enable traps snmp linkup
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless  ap-detection
externalAPDetected
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless  ids excessiveProbes
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless radio adopted
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless self-healing activated
WS5100(config)#
```

```
WS5100(config)#snmp-server enable traps wireless station
tkipCounterMeasures
WS5100(config)#

WS5100(config)#snmp-server enable traps wireless-statistics min-packets
120
WS5100(config)#

WS5100(config)#snmp-server location "Located at thh 5th FLoor"
WS5100(config)#

WS5100(config)#snmp-server sysname "Gold Mine"
WS5100(config)#
```

5.1.25 terminal

Global Configuration Commands

Use this CLI command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no monitor
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults

Usage Guidelines

Example

```
WS5100(config)#terminal monitor
WS5100(config)#
```

5.1.26 timezone

Global Configuration Commands

Use this CLI command to configure the timezone settings of the WS5100 Series Wireless Switch.

Syntax

```
timezone
```

Parameters

TIMEZONE	Press <tab> to traverse list of files. This displays list of files containing timezone information.

Usage Guidelines

Example

```
WS5100(config)#timezone
America/    Asia/       Atlantic/   Australia/  Etc/        Europe/
Pacific/    Africa/

WS5100(config)#timezone America/
America/Anchorage     America/Bogota        America/Buenos_Aires  America/
Caracas       America/Chicago
America/Costa_Rica    America/Denver        America/Los_Angeles   America/
Mexico_City   America/Montreal
America/New_York      America/Phoenix       America/Santiago      America/
Sao_Paulo     America/St_Johns
America/Tegucigalpa   America/Thule         America/Winnipeg      America/
Indianapolis

WS5100(config)#timezone America/Chicago
WS5100(config)#
```

5.1.27 username

Global Configuration Commands

Use this CLI command to establish the user name authentication for the WS5100 Series Wireless Switch.

Syntax

```
username
```

Parameters

WORD	Enter a name to authenticate the WS5100 switch. The username should be between 1 and 28 characters.

Usage Guidelines

Example

```
WS5100(config)#username GoldenSwitch
WS5100(config)#
```

5.1.28 vpn

Global Configuration Commands

Use this CLI command to configure VPN

Syntax

```
vpn authentication-method(local|radius)
```

Parameters

authentication-method	Use this to select the authen
local	Used for user based authentication
radius	Used to radius server authentication

Usage Guidelines

Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

Example

5.1.29 wireless

Global Configuration Commands

Use this CLI command to configure the wireless parameters of the WS5100 Series Wireless Switch. This command will lead you to `config-wireless` instance. For more idetails see *Wireless Instance on page 17-1*.

Syntax

```
wireless
```

Parameters

None.

Usage Guidelines

The wireless command is used to enter the config-wireless instance wherein you can configure the WS5100 wireless parameters. You can confirm that you have entrered the wireless instance as the prompt changes from the the regular `WS5100(config)#` to `WS5100(config-wireless)#.`

Example

```
WS5100(config)#wireless
WS5100(config-wireless)#
```

6

crypto-isakmp

Use `crypto isakmp policy(priority)` to instantiate `config-crypto-isakmp` instance.

6.1 Crypto Isakmp Config commands

Table 6.1 summarizes the **`crypto-isakmp`** commands within the WS5100 Series Switch command line interface

Table 6.1 Trustpoint Config Commands Summary

Command	Description	Ref.
authentication	Set authentication method for protection suite	*page 6-3*
clrscr	Clears the display screen	*page 6-4*
encryption	Set encryption algorithm for protection suite	*page 6-5*
end	End current mode and change to EXEC mode	*page 6-6*
exit	End current mode and down to previous mode	*page 6-7*

Command	Description	Ref.
group	Set the Diffie-Hellman group	*page 6-8*
hash	Set hash algorithm for protection suite	*page 6-9*
help	Description of the interactive help system	*page 6-10*
lifetime	Set lifetime for ISAKMP security association	*page 6-11*
no	Negate a command or set its defaults	*page 6-12*
service	Service Commands	*page 6-13*
show	Show running system information	*page 6-14*

6.1.1 authentication

Use this CLI command to authenticate **`rsa-sig`** and **`pre-share`** keys.

Syntax

```
authentication(pre-share|rsa-sig)
```

Parameters

pre-share	pre shared key
rsa-sig	rsa signature

Example

```
WS5100(config-crypto-isakmp)#authentication pre-share
WS5100(config-crypto-isakmp)#

WS5100(config-crypto-isakmp)#authentication rsa-sig
WS5100(config-crypto-isakmp)#
```

6.1.2 clrscr

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-crypto-isakmp)#clr
WS5100(config-crypto-isakmp)#
```

6.1.3 encryption

Use this CLI command to configure the encryption level of the data transmitted using the WS5100 Wireless Switch using crypto-isakmp command.

Syntax

```
encryption(3des|aes|aes-192|aes-256|des)
```

Parameters

3des	3des - Triple data encryption standard
aes	aes - advanced data encryption standard
aes-192	aes-192 - advanced data encryption standard
aes-256	aes-256 - advanced data encryption standard
des	des - data encryption standard

Example

```
WS5100(config-crypto-isakmp)#encryption 3des
WS5100(config-crypto-isakmp)#

WS5100(config-crypto-isakmp)#encryption aes-256
WS5100(config-crypto-isakmp)#
```

6.1.4 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

```
end
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-crypto-isakmp))#end
WS5100#
```

6.1.5 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-crypto-isakmp)#exit
WS5100(config)#
```

6.1.6 group

Use this CLI command to specify the Diffie-Hellman group (1 or 2) to be used by this IKE policy to generate the keys (which are then used to create the IPSec SA).

Syntax

```
group(1|2|5)
```

Parameters

1	768-bit mod P
2	1024-bit mod P
5	

Usage Guidelines

The local IKE policy and the peer IKE policy must have matching group settings in order for negotiation to be successful.

Example

```
WS5100(config-crypto-isakmp)#group 5
WS5100(config-crypto-isakmp)#
```

6.1.7 hash

Use this CLI command to specify the hash algorithm to be used to authenticate the data transmitted over the IKE SA.

Syntax

```
hash(md5|sha)
```

Parameters

md5	Choose the md5 hash algorithm.
sha	Choose the sha hash algorithm.

Example

```
WS5100(config-crypto-isakmp)#hash sha
WS5100(config-crypto-isakmp)#
```

6.1.8 help

Use thie CLI command to access the systems interactive help system

Syntax

```
help
```

Parameters

None.

Example

```
WS5100(config-crypto-isakmp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-crypto-isakmp)#
```

6.1.9 lifetime

Use this CLI command to specify how long an IKE SA is valid before expiring.

Syntax

```
lifetime <seconds>
```

Parameters

<seconds>	Specify how many seconds an IKE SA will last before expiring.Time stamp in secondscan be configured between 3600 and 2147483647.

Example

```
WS5100(config-crypto-isakmp)#lifetime 5200
WS5100(config-crypto-isakmp)#
```

6.1.10 no

Use this CLI command to negate a command or set its defaults.

Syntax

```
no <previous command used>
```

Parameters

Use the commands that you have configured under this instance.

Example

```
WS5100(config-crypto-isakmp)#no lifetime
WS5100(config-crypto-isakmp)#
```

6.1.11 service

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information
diag-shell	Provide diag shell access
save-cli	Save CLI tree for all modes in html format
show	Show running system information
start-shell	Provide shell access
tethereal	Dump and analyze network traffic

Example

```
WS5100(config-crypto-isakmp)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history

WS5100(config-crypto-isakmp)#service show info
4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.4M out of 18.6M available for crashinfo.

List of Files:
 messages.log                    0       Oct 9  13:01
 snmpd.log                       316     Oct 9  13:01
 startup.log                     16.5k   Oct 9  13:01
 command.history                 7.6k    Oct 9  18:19
 reboot.history                  3.4k    Oct 9  13:01
 upgrade.history                 782     Aug 29 18:32
Please export these files or delete them for more space.
WS5100(config-crypto-isakmp)#
```

6.1.12 show

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-crypto-isakmp)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
```

```
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-crypto-isakmp)#show
```

7

crypto-group

Use `crypto isakmp(client)configuration group default` to initiates `config-crypto-group` instance.

7.1 Crypto Client Config commands

Table 7.1 summarizes the **`config-crypto-group`** commands within the WS5100 Series Switch command line interface

Table 7.1 Trustpoint Config Commands Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 7-3*
dns	Domain Name Server	*page 7-4*
end	End current mode and change to EXEC mode	*page 7-5*
exit	End current mode and down to previous mode	*page 7-6*

Command	Description	Ref.
help	Description of the interactive help system	*page 7-7*
service	Service Commands	*page 7-8*
show	Show running system information	*page 7-9*
wins	Windows name server	*page 7-11*

7.1.1 clrscr

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
WS5100(config-crypto-group)#clr
WS5100(config-crypto-group)#
```

7.1.2 dns

Use this CLIL command to specify the DNS server address(es) to assign to a client.

Syntax

```
dns <IP Address>
```

Parameters

<IP Address>	The first DNS server address to assign.
<IP Address> optional	The second DNS server address to assign.

Example

```
WS5100(config-crypto-group)#dns-server 172.1.17.1 172.1.17.3
WS5100(config-crypto-group)#
```

7.1.3 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-crypto-group)#end
WS5100#
```

7.1.4 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
WS5100(config-crypto-group)#exit
WS5100(config)#
```

7.1.5 help

Use thie CLI command to access the systems interactive help system

Syntax

`help`

Parameters

None.

Example

```
WS5100(config-crypto-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-crypto-group)#
```

7.1.6 service

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information
diag-shell	Provide diag shell access
save-cli	Save CLI tree for all modes in html format
show	Show running system information
start-shell	Provide shell access
tethereal	Dump and analyze network traffic

Example

```
WS5100(config-crypto-group)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
WS5100(config-crypto-group)#service show

WS5100(config-crypto-group)#service show info
4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.4M out of 18.6M available for crashinfo.
List of Files:
 messages.log                    0       Oct 9  13:01
 snmpd.log                       316     Oct 9  13:01
 startup.log                     16.5k   Oct 9  13:01
 command.history                 7.8k    Oct 9  18:46
 reboot.history                  3.4k    Oct 9  13:01
 upgrade.history                 782     Aug 29 18:32
Please export these files or delete them for more space.
WS5100(config-crypto-group)#
```

7.1.7 show

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-crypto-group)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
```

```
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-crypto-group)#show
```

7.1.8 wins

Use this CLIL command to specify the Windows Internet Naming Service (WINS) name servers to assign to a client.

Syntax

```
wins <IP Address> <IP Address>
```

Parameters

<IP Address>	The first WINs server address to assign.
<IP Address> optional	The second WINs server address to assign.

Example

```
WS5100(config-crypto-group)#wins 128.2.11.1 128.2.19.23
WS5100(config-crypto-group)#
```

8

crypto-peer

Use `crypto isakmp(peer)[IP Address|dns|hostname]` to initiates `config-crypto-peer` instance.

8.1 Crypto Peer Config commands

Table 8.1 summarizes the **`config-crypto-peer`** commands within the WS5100 Series Switch command line interface

Table 8.1 Trustpoint Config Commands Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 8-3*
end	End current mode and change to EXEC mode	*page 8-4*
exit	End current mode and down to previous mode	*page 8-5*
help	Description of the interactive help system	*page 8-6*

Command	Description	Ref.
no	Negate a command or set its defaults	*page 8-7*
service	Service Commands	*page 8-8*
set	set	*page 8-9*
show	Show running system information	*page 8-10*

8.1.1 clrscr

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
WS5100(config-crypto-peer)#clr
WS5100(config-crypto-peer)
```

8.1.2 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

```
end
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-crypto-peer)#end
WS5100#
```

8.1.3 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
WS5100(config-crypto-peer)#exit
WS5100(config)#
```

8.1.4 help

Use thie CLI command to access the systems interactive help system

Syntax

```
help
```

Parameters

None.

Example

```
WS5100(config-crypto-peer)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
WS5100(config-crypto-peer)#
```

8.1.5 no

Use this CLI command to negate a command or set its defaults.

Syntax

```
no <previous command used>
```

Parameters

Use the commands that you have configured under this instance.

Example

```
WS5100(config-crypto-peer)#no aggrerssive-mode
WS5100(config-crypto-peer)#
```

8.1.6 service

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information
diag-shell	Provide diag shell access
save-cli	Save CLI tree for all modes in html format
show	Show running system information
start-shell	Provide shell access
tethereal	Dump and analyze network traffic

Example

```
WS5100(config-crypto-peer)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
WS5100(config-crypto-peer)#service show

WS5100(config-crypto-peer)#service show info
4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.4M out of 18.6M available for crashinfo.
List of Files:
 messages.log                    0       Oct 9  13:01
 snmpd.log                       316     Oct 9  13:01
 startup.log                     16.5k   Oct 9  13:01
 command.history                 8.0k    Oct 9  19:26
 reboot.history                  3.4k    Oct 9  13:01
 upgrade.history                 782     Aug 29 18:32
Please export these files or delete them for more space.
WS5100(config-crypto-peer)#
```

8.1.7 set

Use this CLI command to configure the aggressive-mode of **`crypto-peer.`**

Syntax

```
set aggressive-mode (password)
```

Parameters

aggressive-mode	aggressive mode
password	password

Example

```
WS5100(config-crypto-peer)#set aggressive-mode password CheckMeIn
WS5100(config-crypto-peer)#
```

8.1.8 show

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-crypto-peer)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
```

```
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-crypto-peer)#show
```

9

crypto-ipsec

Use the `(config-crypto ipsec)` instance to define the transform configuration for securing data(e.g., esp-3des, esp-sha-hmac, etc.). The transform-set is then assigned to a crypto map using the map's set transform-set command. For more details see crypto-map transform-set *page 10-11*.

9.1 Crypto Ipsec Config commands

Table 9.1 summarizes the **`config-crypto-ipsec`** commands within the WS5100 Series Switch command line interface

Table 9.1 Trustpoint Config Commands Summary

Command	Description	Ref.
clrscr	Clears the display screen	*page 6-4*
end	End current mode and change to EXEC mode	*page 6-6*
exit	End current mode and down to previous mode	*page 6-7*
help	Description of the interactive help system	*page 6-10*

Command	Description	Ref.
mode	IPSec Transporation Mode	*page 9-3*
no	Negate a command or set its defaults	*page 6-12*
service	Service Commands	*page 6-13*
show	Show running system information	*page 9-4*

9.1.1 mode

Use this CLI command to configure the IP Sec transportation mode.

Syntax

```
mode(transport|tunnel)
```

Parameters

transport	Transport Mode
tunnel	Tunnel Mode

Example

```
WS5100(config-crypto-ipsec)#mode transport
WS5100(config-crypto-ipsec)#
```

9.1.2 show

Syntax

```
clrscr
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-crypto-ipsec)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
```

```
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

WS5100(config-crypto-ipsec)#show
```

10

crypto-map

`config-crypto-map` CLI commands are used to define a Certificate Authority (CA) trustpoint. This is a seperate instance by itself but belongs to the `crypto pki trustpoint` mode under `config` instance.

10.1 Trustpoint Config commands

Table 10.1 summarizes the **`config-crypto-map`** commands within the WS5100 Series Switch command line interface

Table 10.1 Trustpoint Config Commands Summary

Command	Description	Ref.
clrscr	Clears the display screen	
end	End current mode and change to EXEC mode	
exit	End current mode and down to previous mode	
help	Description of the interactive help system	

Command	Description	Ref.
match	Match values	
no	Negate a command or set its defaults	
service	Service Commands	
set	Set values for encryption/decryption	
show	Show running system information	

10.1.1 clrscr

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
WS5100(config-crypto-map)#clr
WS5100(config-crypto-map)
```

10.1.2 end

Use this CLI command to end and exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

```
end
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-crypto-map)#end
WS5100#
```

10.1.3 exit

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
WS5100(config-crypto-map)#exit
WS5100(config)#
```

10.1.4 help

Use thie CLI command to access the systems interactive help system

Syntax

```
help
```

Parameters

None.

Example

```
WS5100(config-crypto-map)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
WS5100(config-crypto-map)#
```

10.1.5 match

Use this CLI command to assign an IP access-list to a crypto map definition. The access-list designates the IP packets to be encrypted by this crypto map.

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike. Each entry is given an index, which is used to sort the ordered list.

When a non-secured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable SA exists, that is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists, and the crypto map entry is "respond only", the packet is discarded.

When a secured packet arrives on an interface, its SPI is used to look up an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

Syntax

```
match <list name>
```

Parameters

list name	Enter the name of the access-list or acl-id you wish to assign to this crypto map.

Usage Guidelines

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An access control list (ACL) is assigned to the crypto map using the match address command (see crypto map on page 151). If no ACL is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the OS product. The source information must be the local OS product and the destination must be the peer.

Only extended access-lists can be used in crypto maps.

Example

The following example shows setting up an ACL (called TestList) and then assigning the new list to a crypto map (called TestMap):

```
WS5100(config)#ip access-list extended TestList
Configuring New Extended ACL "TestList"
(config-ext-nacl)#exit

WS5100(config)#crypto map TestMap 220 isakmp dynamic
WS5100(config-crypto-map)#

WS5100(config-crypto-map)#match address TestMap
WS5100(config-crypto-map)#
```

10.1.6 no

Use this CLI command to negate a command or set its defaults.

Syntax

```
no <previous command used>
```

Parameters

Use the commands that you have configured under this instance.

Example

```
WS5100(config-crypto-map)#no aggrerssive-mode
WS5100(config-crypto-map)#
```

10.1.7 service

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-crypto-isakmp)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information
diag-shell	Provide diag shell access
save-cli	Save CLI tree for all modes in html format
show	Show running system information
start-shell	Provide shell access
tethereal	Dump and analyze network traffic

Example

```
WS5100(config-crypto-map)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
WS5100(config-crypto-map)#service show

WS5100(config-crypto-map)#service show info
4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.4M out of 18.6M available for crashinfo.
List of Files:
 messages.log                    0       Oct 9  13:01
 snmpd.log                       316     Oct 9  13:01
 startup.log                     16.5k   Oct 9  13:01
 command.history                 8.5k    Oct 9  20:26
 reboot.history                  3.4k    Oct 9  13:01
 upgrade.history                 782     Aug 29 18:32
Please export these files or delete them for more space.
WS5100(config-crypto-map)#
```

10.1.8 set

Use this CLI command to set the various set parameters of the peer device.

Syntax

```
set (localid|mode|peer|pfs|security-association|session-key|transformset)
set localid(IP Address|dn|hostname)

set security-association
(level(perhost)|lifetime(kilobytes|seconds)<value>)

set session-key (inbound|outbound)(ah|esp)
set session-key (inbound|outbound) ah <hexkey data>
set session-key (inbound|outbound) esp <SPI> cipher <hexdata key>
authenticator <hexkey data>
```

Parameters

localid	
address	
dn	
hostname	
mode	
aggressive	aggressive mode
main	main mode
peer	Use the set peer command to set the IP address of the peer device. This can be set for multiple remote peers. Remote peer can be either in IP Address or hostname. **NOTE** For manual mode, only one remote peer can be added for crypto map.
IP address	Enter the IP address of the peer device. If this is not configured, it implies responder only to any peer.
pfs	Use the set pfs command to choose the type of perfect forward secrecy (if any) that will be required during IPSec negotiation of security associations for this crypto map. Use the no form of this command to require no PFS.

group 1	IPSec is required to use Diffie-Hellman Group 1 (768-bit modulus) exchange during IPSec SA key generation.
group 2	IPSec is required to use Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPSec SA key generation.
group 5	IPSec is required to use Diffie-Hellman Group 5
security-association	Use the set security-association lifetime command to define the lifetime (in kilobytes and/or seconds) of the IPSec SAs created by this crypto map.
level(perhost)	ipsec sa level
lifetime(kilobyte|seconds)	ipsec sa lifetime. • kilobytes – SA lifetime limit in kilobytes. • seconds – SA lifetime limit in seconds
session-key	Use the set session-key command to define the encryption and authentication keys for this crypto map.
inbound	Use this keyword to define encryption keys for inbound traffic.
outbound	Use this keyword to define encryption keys for outbound traffic.
ah	Authentication header protocol
esp	Encapsulating security payload protocol.
SPI	Security Parameter Index
cipher *<hex key data>*	Specify encryption/decryption key.
authenticator *<hex key data>*	Specify authentication key.
transformset <name>	Use the set transform-set command to assign a transform-set to a crypto map.

Usage Guidelines

WS5100(config-crypto-map)#set peer (name)

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first; then the new peer IP address can be configured.

WS5100(config-crypto-map)#set pfs

If left at the default setting, no perfect forward secrecy (PFS) will be used during IPSec SA key generation. If PFS is specified, then the specified Diffie-Hellman Group exchange will be used for the initial and all subsequent key generation, thus providing no data linkage between prior keys and future keys.

WS5100(config-crypto-map)#set security-association lifetime (kilobytes|seconds)

Values can be entered for this command in both kilobytes and seconds. Whichever limit is reached first will end the security association.

WS5100(config-crypto-map)#set session-key (inbound|outbound)(ah|esp)

WS5100(config-crypto-map)#set session-key (inbound|outbound) ah <hexkey data>

WS5100(config-crypto-map)#set session-key (inbound|outbound) esp <SPI> cipher <hexdata key> authenticator <hexkey data>

The inbound local SPI (security parameter index) must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys.

They are not true ASCII strings. Therefore, a key of 3031323334353637 represents "01234567".

WS5100(config-crypto-map)#set transformset (name)

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms (see crypto ipsec transform-set <setname> <parameters> on page 150).

If no transform-set is configured for a crypto map, then the entry is incomplete and will have no effect on the system. For manual key crypto maps, only one transform set can be specified.

Example

```
WS5100(config-crypto-map)#set localid hostname TestMapHost
WS5100(config-crypto-map)#
```

10.1.9 show

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-crypto-map)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
```

```
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-crypto-map)#show
```

11

crypto-trustpoint Instance

`config-crypto-trustpoint` CLI commands are used to define a Certificate Authority (CA) trustpoint. This is a seperate instance by itself but belongs to the `crypto pki trustpoint` mode under `config` instance.

11.1 Trustpoint Config commands

Table 11.1 summarizes the **`config-crypto-trustpoint`** commands within the WS5100 Series Switch command line interface

Table 11.1 Trustpoint Config Commands Summary

Command	Description	Ref.
clrscr	Clears the display screen	page 11-3
company-name	Company Name(Applicable only for request)	page 11-4
email	email	page 11-5

Command	Description	Ref.
end	End current mode and change to EXEC mode	page 11-6
exit	End current mode and down to previous mode	page 11-7
fqdn	Domain Name Configuration	page 11-8
help	Description of the interactive help system	page 11-9
ip-address	Internet Protocol (IP)	page 11-10
no	Negate a command or set its defaults	page 11-11
password	Challenge Password(Applicable only for request)	page 11-12
rsakeypair	Rsa Keypair to associate with the trustpoint	page 11-13
service	Service Commands	page 11-14
show	Show running system information	page 11-16
subject-name	Subject Name is a collection of required parameters to configure a trustpoint.	page 11-18

11.1.1 clrscr

Trustpoint Config commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#clrscr
WS5100(config-trustpoint)#
```

11.1.2 company-name

Trustpoint Config commands

Company Name(Applicable only for request)

Syntax

```
company-name
```

Parameters

WORD	Company Name(2 to 64 characters)

Usage Guidelines

Example

```
WS5100(config-trustpoint)#company-name RetailKing
WS5100(config-trustpoint)#
```

11.1.3 email

Trustpoint Config commands

Use this CLI command to configure you e-mail ID for the trustpoint.

Syntax

```
email
```

Parameters

WORD	email address(2 to 64 characters)

Usage Guidelines

Example

```
WS5100(config-trustpoint)#email abcTestemailID@symbol.com
WS5100(config-trustpoint)#
```

11.1.4 end

Trustpoint Config commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#.`

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#end
WS5100#
```

11.1.5 exit

Trustpoint Config commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#exit
WS5100(config)#
```

11.1.6 fqdn

Trustpoint Config commands

Use this CLI command to configure the domain name of the trustpoint.

Syntax

```
fqdn
```

Parameters

None

Usage Guidelines

Example

```
WS5100(config-trustpoint)#fqdn RetailKing.com
WS5100(config-trustpoint)#
```

11.1.7 help

Trustpoint Config commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-trustpoint)#
```

11.1.8 ip-address

Trustpoint Config commands

Use this CLI command to configure a IP adress for the trustpoint.

Syntax

```
ip-address
```

Parameters

A.B.C.D	Enter the IP address to be configured for the trustpoint.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#ip-address 157.200.200.02
WS5100(config-trustpoint)#
```

11.1.9 no

Trustpoint Config commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no <previous command used>
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#no ip-address
WS5100(config-trustpoint)#
```

11.1.10 password

Trustpoint Config commands

Use this CLI command to set the challenge password, applicable only for requests, to acces trustpoint.

Syntax

```
password(0|2|WORD)
```

Parameters

0	Password is specified UNENCRYPTED. The password should be between 4 to 20 characters.
2	Password is encrypted with password-encryption secret.The string length of encrypted password should be of 44 to 64 characters.
WORD	Password(4 to 20 characters)

Usage Guidelines

Example

```
WS5100(config-trustpoint)#password 0 TestPassword
WS5100(config-trustpoint)#
```

11.1.11 rsakeypair

Trustpoint Config commands

Use thie CLI command to configure a RSA Keypair to associate with the trustpoint.

Syntax

```
rsakeypair
```

Parameters

WORD	Rsa Keypair Identifier

Usage Guidelines

RSA Key Pair Support feature allows you to configure WS5100 Sereies Wireless Switch to have Rivest, Shamir, and Adelman (RSA) key pairs. Thus, the WS5100 Series Wireless Switch software can maintain a different key pair for each identity certificate.

Example

11.1.12 service

Trustpoint Config commands

Use this CLI command to invoke the service commands to trobuleshoot or debug the `crypto pki trustpoint` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information.
diag-shell	Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Show running system information.
start-shell	Provide shell access.
tethereal	Dump and analyze network traffic.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#service diag-shell

Diagnostic shell started for testing
diag >
  boot            Reboots the switch
  delete          Deletes specified file from the system.
  exit            Exit from the CLI
  fallback        Configures firmware fallback feature
  help            Description of the interactive help system
  logout          Exit from the CLI
  no              Negate a command or set its defaults
  reload          Halt and perform a warm reboot
  service         Service Commands
  show            Show running system information
  upgrade         Upgrade firmware image
```

```
diag >
WS5100(config-trustpoint)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history

WS5100(config-trustpoint)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:

WS5100(config-trustpoint)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp packet
only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]
```

11.1.13 show

Trustpoint Config commands

Use thie CLI command to view the current system information t hat is running on the WS5100 Series Wirteless Switch.

Syntax

```
show <parameter>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
```

```
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-trustpoint)#show access-list
Standard IP access list 1
    deny any rule-precedence 1
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
   1       cli    Console           06:12m      Jan  1 00:00:00 1970
** 2       cli    157.235.206.39    00:00m      Jan  1 00:00:00 1970
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#show users
   Line       PID   User        Uptime      Location
   0 con 0  306               06:14:07     ttyS0
 130 vty 0  2744               00:25:49     0
WS5100(config-trustpoint)#

WS5100(config-trustpoint)#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Aug 29 18:32:17 2006
WS5100(config-trustpoint)#
```

11.1.14 subject-name

Trustpoint Config commands

Use this CLI to create a subject name to configure a trustpoint. Subject name is a collection of required parameters to configure a trustpoint.

Syntax

```
subject-name
```

Parameters

WORD	Enter a brief description as prompted by the parameter.

Usage Guidelines

Example

```
WS5100(config-trustpoint)#subject-name TestPool ?
  WORD  Country ( 2 character ISO Code )

WS5100(config-trustpoint)#subject-name TestPool US ?
  WORD  State( 2 to 128 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH ?
  WORD  City( 2 to 128 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH PB ?
  WORD  Organization( 2 to 64 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH PB SYMBOL ?
  WORD  Organization Unit( 2 to 64 characters )

WS5100(config-trustpoint)#subject-name TestPool US OH PB SYMBOL WID ?
  <cr>

WS5100(config-trustpoint)#subject-name TestPool US OH PB SYMBOL WID
WS5100(config-trustpoint)#
```

12 interface Instance

Use **(config-if)** instance to configure the interfaces — ethernet,vlan and tunnel associated with the WS5100 Series Wireless Switch.

12.1 Interface Config commands

Table 12.1 summarizes the **config-if** commands within the WS5100 Series Switch command line

Table 12.1 Interface Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	page 12-3
crypto	crypto	page 12-4
description	Interface specific description	page 12-5
duplex	Set duplex to interface	page 12-6

Command	Description	Ref.
end	End current mode and change to EXEC mode	page 12-7
exit	End current mode and down to previous mode	page 12-8
help	Description of the interactive help system	page 12-9
ip	Internet Protocol (IP)	page 12-10
management	Sets the selected interface as management interface	page 12-11
mtu	Set mtu value for vlan interface	page 12-12
no	Negate a command or set its defaults	page 12-13
service	Service Commands	page 12-14
show	Show running system information	page 12-17
shutdown	Shutdown the selected interface	page 12-20
speed	Configure speed	page 12-21
switchport	Set switching mode characteristics	page 12-22
terminal	Set terminal line parameters	page 12-24
tunnel	protocol-over-protocol tunneling	page 12-25

12.1.1 clrscr

Interface Config commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-if)#clrscr
WS5100(config-if)#
```

12.1.2 crypto

Interface Config commands

Syntax

`crypto map``(WORD)`

Parameters

map	
WORD	

Usage Guidelines

At any given instance you can add only one crypto mapset to one interface. WS5100 wireless switch does not support the same cryptomap set to be attached to multiple interfaces.

Example

```
EXAMPLE OUTPUT HERE
```

12.1.3 description

Interface Config commands

Use this CLI command to create an interface specific desciption.

Syntax

```
description
```

Parameters

LINE	Characters describing this interface

Usage Guidelines

Example

```
WS5100(config-if)#description "interface for RetailKing"
WS5100(config-if)#
```

12.1.4 duplex

Interface Config commands

Use thsi CLI command to configure a duplex type to the interface.

NOTE

- Duplexity can only be set for Ethernet type Interface.You need to enter the `(config-if)` instance using `eth` parameter of `interface` mode.
- Duplex can not be set until speed is set to non-auto value

Syntax

```
duplex(auto|full|half)
```

Parameters

auto	set auto-negotiate
full	set full-duplex
half	set half-duplex

Usage Guidelines

Example

12.1.5 end

Interface Config commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-if)#end
WS5100#
```

12.1.6 exit

Interface Config commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-if)#exit
WS5100(config)#
```

12.1.7 help

Interface Config commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-if)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-if)#
```

12.1.8 ip

Interface Config commands

Use this CLI command to configure the IP address for the assigned ethernet, VLAN or tunnel.

Syntax

```
ip(access-group|address|helper-address|nat)
ip access-group(<1-99>|<100-199>|<1300-1999>|<2000-2699>)in
ip address(A.B.C.D/M|dhcp)
ip helper-address A.B.C.D
ip nat(inside|outside)
```

Parameters

access-group	Access group
(*<1-99>*|*<100-199>*)	IP extended access list
(*<1300-1999>*|*<2000-2699>*)	IP extended access list (expanded range)
WORD	Access List Name
in	Incoming packets
address	Set the IP address of an interface
A.B.C.D/M	IP address (e.g. 10.0.0.1/8)
dhcp	Use DHCP Client to obtain IP address for this interface
helper-address	Forward DHCP and BOOTP packets
A.B.C.D	IP to which DHCP and BOOTP packets are forwarded
nat	Network Address Translation (NAT)
inside	Inside interface
outside	Outside interface

Usage Guidelines

Example

12.1.9 management

Interface Config commands

Use this CLI command to configure the selected interface as management interface.

Syntax

```
management
```

Parameters

None.

Usage Guidelines

Example

12.1.10 mtu

Interface Config commands

Use this CLI command to set the mtu value for an VLAN interface.

NOTE This command is valid only with an VLAN interface.

Syntax

```
mtu <512-1500>
```

Parameters

<512-1500>	Value of MTU in bytes.

Usage Guidelines

Example

```
WS5100(config)#interface vlan 20

WS5100(config-if)#mtu 520
WS5100(config-if)#
```

12.1.11 no

Interface Config commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no <previous command used>
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-if)#no mtu
WS5100(config-if)#
```

12.1.12 service

Interface Config commands

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-if)` instance configurations.

Syntax

```
service(ap|clear|diag-shell|save-cli|show|start-shell|tethereal|wireless)
service ap force-dump
```

Parameters

ap	access-port serviceability parameters
force-dump	trigger the access-port to send a crash-dump to the wireless-switch.
clear	Remove specified support information.
diag-shell	Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Show running system information.
start-shell	Provide shell access.
tethereal	Dump and analyze network traffic.
wireless	Wireless parameters

Usage Guidelines

Example

```
WS5100(config-if)#service ap force-dump
WS5100(config-if)#
```

```
WS5100(config-if)#service diag-shell

Diagnostic shell started for testing

diag >
  boot            Reboots the switch
  delete          Deletes specified file from the system.
  exit            Exit from the CLI
  fallback        Configures firmware fallback feature
  help            Description of the interactive help system
  logout          Exit from the CLI
  no              Negate a command or set its defaults
  reload          Halt and perform a warm reboot
  service         Service Commands
  show            Show running system information
  upgrade         Upgrade firmware image

diag >

WS5100(config-if)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
WS5100(config-if)#

WS5100(config-if)#service show ?
  ap               access-port serviceability parameters
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
  wireless         Wireless parameters

WS5100(config-if)#service show

WS5100(config-if)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:

WS5100(config-if)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
```

```
        [-i <interface on which to capture packets> ] [-W (wisp packet
only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]

WS5100(config-if)#service tethereal

WS5100(config-if)#service wireless ?
  dump-core         Create a core file of the ccsrvr process
  dump-state        Create a ccsrvr.dump file in nvram with internal state
                    information
  mu-history        Enable mu association history
  mu-history-clear  Delete all mu association history files
  rate-scale        Enable wireless rate scaling (default)
  request-ap-log    Request ap Log

WS5100(config-if)#service wireless request-ap-log 1 ?
  file  output to file
  log   output to syslog
WS5100(config-if)#
```

12.1.13 show

▶ *Interface Config commands*

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

Example

```
WS5100(config-if)#show ?
  access-list           Internet Protocol (IP)
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                crypto
  debugging             Display debugging setting
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status and configuration
  ip                    Internet Protocol (IP)
  ldap                  ldap server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Media Access Control
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
```

```
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-if)#show

WS5100(config-if)#show access-list
Standard IP access list 1
    deny any rule-precedence 1
WS5100(config-if)#

WS5100(config-if)#show boot

Image           Build Date              Install Date           Version
-----       --------------------    --------------------      -----------
--
Primary     Aug 28 14:05:16 2006     Aug 29 18:32:17 2006     3.0.0.0-200B
Secondary   Aug 14 06:18:03 2006     Aug 17 15:08:28 2006     3.0.0.0-180B

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
WS5100(config-if)#

WS5100(config-if)#show wireless ?
  ap                          Status of adopted access-port
  ap-detection-config         Detected-AP Configuration Parameters
  ap-images                   List of access-port images on the wireless
                              switch
  ap-unadopted                List of unadopted access-port
  approved-aps                Approved APs seen by access-port scans
  channel-power               List of available channel and power levels
for
                              a radio
  config                      Wireless Configuration Parameters
  hotspot-config              Wlan hotspot configuration
  ids                         Intrusion detection parameters
  mac-auth-local              list out the mac-auth-local entries
  mobile-unit                 Details of associated mobile-units
```

```
  phrase-to-key               display the WEP keys generated by a
passphrase
  qos-mapping                 Quality of Service mappings used for mapping
                              WMM access categories and 802.1p / DSCP tags
  radio                       Radio related commands
  regulatory                  Regulatory (allowed channel/power)
information
                              for a particular country
  self-heal-config            Self-Healing Configuration Parameters
  sensor                      Wireless Intrusion Protection System
parameters
  unapproved-aps              Unapproved APs seen by access-port or
                              mobile-unit scans
  wireless-switch-statistics  wireless-switch  statistics
  wlan                        Wireless LAN related parameters

WS5100(config-if)#

WS5100(config-if)#show wireless config
country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
dot11-shared-key-auth   : disabled
ap-detection            : disabled
oversized-frames        : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp fix windows        : disabled
broadcast-tx-speed      : optimize-for-throughput
smart-scan 11a channels :
smart-scan 11bg channels:
WS5100(config-if)#
```

12.1.14 shutdown

Interface Config commands

Use thie CLI command to shutdown the selected interface.

Syntax

```
shutdown
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-if)#shutdown
WS5100(config-if)#
```

12.1.15 speed

Interface Config commands

Use this CLI command to configure the speed of the selected interface in Mbps.

Syntax

```
speed(10|100|1000|auto)
```

Parameters

10	Force 10 Mbps operation
100	Force 100 Mbps operation
1000	Force 1000 Mbps operation
auto	Enable AUTO speed configuration

Usage Guidelines

Example

```
WS5100(config-if)#speed auto
WS5100(config-if)#
```

12.1.16 switchport

Interface Config commands

Use this CLI command to set switching mode characteristics of the selected interface.

Syntax

```
switchport(access|mode|trunk)
switchport access vlan <1-4094>
switchport mode(access|trunk)
switchport trunk(allowed|native)
switchport trunk allowed vlan(add|none|remove)[VLAN_ID]
switchport trunk native(tagged|vlan<1-4094>)
```

Parameters

access	Set access mode characteristics
vlan	Set VLAN when interface is in access mode
<1-4094>	Access VLAN ID
mode	Set the mode of the Layer2 interface
access	Set the Layer2 interface as access
trunk	Set the Layer2 interface as trunk
trunk	Set trunking mode characteristics
(allowed)	Set trunking mode allowed vlan characteristics
vlan	Set the allowed VLANs
add	add VLANs to the current list
none	Allow no VLANs to Xmit/Rx through the Layer2 interface
remove	Remove VLANs from the current list
VLAN_ID	The List of the VLAN IDs that will be added/removed. e.g. 10-20,25,30-35
(native)	Set native trunking characteristics
tagged	Tag the native vlan
vlan	Set the native VLAN for classifying untagged traffic
<1-4094>	The native VLAN id when interface is in trunking mode

Usage Guidelines

Example

```
WS5100(config-if)#switchport mode access
WS5100(config-if)#
```

12.1.17 terminal

Interface Config commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults
monitor	Copy debug output to the current terminal line

Usage Guidelines

Example

```
WS5100(config-if)#terminal no monitor
\WS5100(config-if)#\

\WS5100(config-if)#terminal monitor
WS5100(config-if)#
```

12.1.18 tunnel

Interface Config commands

Use this CLI command to configure protocol-over-protocol tunneling.

Syntax

```
tunnel(destination|source|ttl)
tunnel destination A.B.C.D
tunnel source A.B.C.D
tunnel ttl<1-255>
```

Parameters

destination	destination of tunnel packets
source	source of tunnel packets
A.B.C.D	Internet Protocol (IP)
ttl	set time to live
<1-255>	ttl in seconds.

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

13

Extended ACL Instance

Use **(config-ext-nacl)** instance to configure the **ip access-list extended** ACLs associated with the WS5100 Series Wireless Switch.

13.1 Extended ACL Config Commands

Table 13.1 summarizes the **config-ext-nacl** commands within the WS5100 Series Switch command line

Table 13.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	page 13-3
deny	Specify packets to reject	page 13-4
end	End current mode and change to EXEC mode	page 13-6
exit	End current mode and down to previous mode	page 13-7

Command	Description	Ref.
help	Description of the interactive help system	page 13-8
mark	Specify packets to mark	page 13-9
no	Negate a command or set its defaults	page 13-11
permit	Specify packets to forward	page 13-12
service	Service Commands	page 13-14
show	Show running system information	page 13-16
terminal	Set terminal line parameters	page 13-18

13.1.1 clrscr

Extended ACL Config Commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-nacl)#clrscr
WS5100(config-ext-nacl)#
```

13.1.2 deny

Extended ACL Config Commands

Use this CLI command to specify packets that you want to reject.

Syntax

```
deny(icmp|ip|tcp|udp)

deny icmp(Source IP Address)(Destination Address)
(<0-255>|log|rule-precedence<1-5000>|wlan<1-32>)

deny icmp(Source IP Address)(Destination Address)
log rule-precedence<1-5000>

deny icmp(Source IP Address)(Destination Address)
rule-precedence<1-5000>

deny icmp(Source IP Address)(Destination Address)
wlan<1-32> log rule-precedence<1-5000>
```

Syntax

```
deny ip (Source IP Address)(Destination IP Address)
(log|rule-precedence<1-500>|wlan<1-32>)

deny ip (Source IP Address)(Destination IP Address)
log rule-precedence<1-500>

deny ip (Source IP Address)(Destination IP Address)
rule-precedence<1-500>

deny ip (Source IP Address)(Destination IP Address)
wlan<1-32> log rule-precedence<1-500>
```

Syntax

```
deny (tcp|udp) (Source IP Address)(Destination IP Address)

deny (tcp|udp) (Source IP Address)(Destination IP Address) log

deny (tcp|udp) (Source IP Address)(Destination IP Address) log wlan <1-32>

deny (tcp|udp) (Source IP Address)(Destination IP Address) log
rule-precedence <1-5000>

deny (tcp|udp) (Source IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)

deny (tcp|udp)(Source IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)log
```

```
deny (tcp|udp)(Source IP Address) (eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
log wlan <1-32>

deny (tcp|udp)(Source IP Address) (eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
log rule-precedence <1-5000>
```

Parameters

icmp	ICMP Protocol
ip	Any Internet Protocol
Source IP	Source IP address can be one of the following: • A.B.C.D/M – Source IP address range to match • any – Any source IP address • host – Single host address
Destination IP	Destination IP address can be one of the following: • A.B.C.D/M – Destination IP address range to match • any – Any destination IP address • host – Single host address
<0-255>	ICMP Type
log	Log matches against this entry
rule-precedence*<1-5000>*	Access-list entry precedence
wlan*<1-32>*	Filter packets based on WLAN
eq*<1-65535>*	Match a specific destination port
range*<1-65535> <1-65535>*	Match a range of destination ports. You can select between Starting destination port and Ending destination port.

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

13.1.3 end

Extended ACL Config Commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-nacl)#end
WS5100#
```

13.1.4 exit

Extended ACL Config Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-nacl)#exit
WS5100(config)#
```

13.1.5 help

Extended ACL Config Commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-ext-nacl)#
```

13.1.6 mark

Extended ACL Config Commands

Use this CLI command to specify packet that you want to mark.

Syntax

```
mark(8021p|tos)(<0-7>|<0-255>)(icmp|ip|tcp|udp)
(Source IP Address)(Destination IP Address)

mark(8021p|tos)(<0-7>|<0-255>) icmp(Source IP Address)
(Destination IP Address)(<0-255>|log|wlan<1-32> rule-precedence<1-5000>
```

Syntax

```
mark(8021p|tos)(<0-7>|<0-255>) ip(Source IP Address)
(Destination IP Address)(log|rule-precedence|wlan)log

mark(8021p|tos)(<0-7>|<0-255>) ip(Source IP Address)
(Destination IP Address)(log|rule-precedence|wlan)
log rule-precedence<1-500>

mark(8021p|tos)(<0-7>|<0-255>) ip(Source IP Address)
(Destination IP Address)(log|wlan) rule-precedence<1-500>

mark(8021p|tos)(<0-7>|<0-255>) ip(Source IP Address)
(Destination IP Address)(log|rule-precedence|wlan|A.B.C.D)wlan<1-32> log
rule-precedence<1-500>
```

Syntax

```
mark(8021p|tos)(<0-7>|<0-255>)(tcp|udp)(Source IP Address)
(Destination IP Address)(eq<1-65535>|log|range<1-65535> <1-65535>|
rule-precedence<1-5000>|wlan<1-32>)

mark(8021p|tos)(<0-7>|<0-255>)(tcp|udp)(Source IP Address)
(Destination IP Address)(eq<1-65535>|log|range<1-65535> <1-65535>|
rule-precedence<1-5000>|wlan<1-32>) log

mark(8021p|tos)(<0-7>|<0-255>)(tcp|udp)(Source IP Address)
(Destination IP Address)(eq<1-65535>|log|range<1-65535> <1-65535>|
rule-precedence<1-5000>|wlan<1-32>) log wlan<1-32>

mark(8021p|tos)(<0-7>|<0-255>)(tcp|udp)(Source IP Address)
(Destination IP Address)(eq<1-65535>|log|range<1-65535> <1-65535>|
rule-precedence<1-5000>|wlan<1-32>) log rule-precedence<1-5000>
```

Parameters

8021p <0-7>	Modify 802.1p VLAN user priority
tos <0-255>	Modify TOS bits in IP header
icmp	ICMP Protocol
ip	Any Internet Protocol
tcp	TCP Protocol
udp	UDP Protocol
Source IP Address	Source IP address can be one of the following: • `A.B.C.D/M` – Source IP address range to match • `any` – Any source IP address • `host` – Single host address
Destination IP Address	Destination IP address can be one of the following: • `A.B.C.D/M` – Destination IP address range to match • `any` – Any Destination IP address • `host` – Single host address
<0-255>	ICMP Type
log	Log matches against this entry
rule-precedence*(1-5000)*	Access-list entry precedence
wlan*(1-32)*	Filter packets based on WLAN
eq *<1-65535>*	Match a specific source port
range*<1-65535> <1-65535>*	Match a range of source ports

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

13.1.7 no

Extended ACL Config Commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no(deny|mark|permit)
```

This command negates all the syntax combinatins that you have used in *deny*, *mark* and *permit* to configure the Extended ACL.

Parameters

deny	Specify packets to reject
mark	Specify packets to mark
permit	Specify packets to forward

Usage Guidelines

Example

13.1.8 permit

▶ *Extended ACL Config Commands*

Syntax

```
permit(icmp|ip|tcp|udp)

permit icmp(Source IP Address)(Destination Address)
(<0-255>|log|rule-precedence<1-5000>|wlan<1-32>)

permit icmp(Source IP Address)(Destination Address)
log rule-precedence<1-5000>

permit icmp(Source IP Address)(Destination Address)
rule-precedence<1-5000>

permit icmp(Source IP Address)(Destination Address)
wlan<1-32> log rule-precedence<1-5000>
```

Syntax

```
permit ip (Source IP Address)(Destination IP Address)
(log|rule-precedence<1-500>|wlan<1-32>)

permit ip (Source IP Address)(Destination IP Address)
log rule-precedence<1-500>

permit ip (Source IP Address)(Destination IP Address)
rule-precedence<1-500>

permit ip (Source IP Address)(Destination IP Address)
wlan<1-32> log rule-precedence<1-500>
```

Syntax

```
permit(tcp|udp)(Source IP Address)(Destination IP Address)

permit(tcp|udp)(Source IP Address)(Destination IP Address) log

permit(tcp|udp)(Source IP Address)(Destination IP Address) log wlan <1-32>

permit(tcp|udp)(Source IP Address)(Destination IP Address) log
rule-precedence <1-5000>

permit(tcp|udp)(Source IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)

permit(tcp|udp)(Source IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)log
```

```
permit(tcp|udp)(Source IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
log wlan <1-32>

permit(tcp|udp)(Source IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
(Destination IP Address)(eq <1-65535>|range <1-65535> <1-65535>)
log rule-precedence <1-5000>
```

Parameters

icmp	ICMP Protocol
ip	Any Internet Protocol
Source IP	Source IP address can be one of the following: • A.B.C.D/M – Source IP address range to match • any – Any source IP address • host – Single host address
Destination IP	Destination IP address can be one of the following: • A.B.C.D/M – Destination IP address range to match • any – Any destination IP address • host – Single host address
<0-255>	ICMP Type
log	Log matches against this entry
rule-precedence*<1-5000>*	Access-list entry precedence
wlan*<1-32>*	Filter packets based on WLAN
eq*<1-65535>*	Match a specific destination port
range*<1-65535> <1-65535>*	Match a range of destination ports. You can select between Starting destination port and Ending destination port.

Usage Guidelines

Example

13.1.9 service

Extended ACL Config Commands

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-if)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information.
diag-shell	Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Show running system information.
start-shell	Provide shell access.
tethereal	Dump and analyze network traffic.

Usage Guidelines

Example

```
WS5100(config-ext-nacl)#service diag-shell

Diagnostic shell started for testing

diag >
  boot            Reboots the switch
  delete          Deletes specified file from the system.
  exit            Exit from the CLI
  fallback        Configures firmware fallback feature
  help            Description of the interactive help system
  logout          Exit from the CLI
  no              Negate a command or set its defaults
  reload          Halt and perform a warm reboot
  service         Service Commands
  show            Show running system information
  upgrade         Upgrade firmware image

diag >
```

```
WS5100(config-ext-nacl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
WS5100(config-ext-nacl)#

WS5100(config-ext-nacl)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history

WS5100(config-ext-nacl)#service show

WS5100(config-ext-nacl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:

WS5100(config-ext-nacl)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp packet
only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]

WS5100(config-ext-nacl)#service tethereal
```

13.1.10 show

Extended ACL Config Commands

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show<paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

Example

```
WS5100(config-ext-nacl)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
```

```
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-ext-nacl)#show
```

13.1.11 terminal

Extended ACL Config Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults
monitor	Copy debug output to the current terminal line

Usage Guidelines

Example

```
WS5100(config-ext-nacl)#terminal monitor
WS5100(config-ext-nacl)#

WS5100(config-ext-nacl)#terminal no monitor
WS5100(config-ext-nacl)#
```

14

Standard ACL Instance

Use **(config-std-nacl)** instance to configure the **ip access-list standard** ACLs associated with the WS5100 Series Wireless Switch.

14.1 Standard ACL Config Commands

Table 14.1 summarizes the **config-std-nacl** commands within the WS5100 Series Switch command line

Table 14.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	page 14-3
deny	Specify packets to reject	page 14-4
end	End current mode and change to EXEC mode	page 14-5
exit	End current mode and down to previous mode	page 14-6

Command	Description	Ref.
help	Description of the interactive help system	page 14-7
mark	Specify packets to mark	page 14-8
no	Negate a command or set its defaults	page 14-9
permit	Specify packets to forward	page 14-10
service	Service Commands	page 14-11
show	Show running system information	page 14-13
terminal	Set terminal line parameters	page 14-15

14.1.1 clrscr

Standard ACL Config Commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-std-nacl)#clrscr
WS5100(config-std-nacl)#
```

14.1.2 deny

Standard ACL Config Commands

Use this CLI command to specify packets that you want to reject.

Syntax

```
deny(A.B.C.D/M|any|host)
deny any(log|rule-precedence|wlan)
deny any log(rule-precedence)<1-500>
deny any rule-precedence<1-500>
deny any wlan<1-32>(log|rule-precedence)(rule-precedence)<1-500>
deny host A.B.C.D
```

Parameters

A.B.C.D/M	Source IP address range to match
any	Any source IP address
log	Log matches against this entry
rule-precedence<*1-500*>	Access-list entry precedence
<*1-500*>	Precedence Value
wlan<*1-32*>	Filter packets based on WLAN
<*1-32*>	WLAN index
host	Single host address
A.B.C.D	Exact source IP address to match

Usage Guidelines

Example

```
WS5100(config-std-nacl)#deny any log rule-precedence 50
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#deny any rule-precedence 60
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#deny any wlan 30 log rule-precedence 250
WS5100(config-std-nacl)#
```

14.1.3 end

Standard ACL Config Commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-std-nacl)#end
WS5100#
```

14.1.4 exit

Standard ACL Config Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-std-nacl)#exit
WS5100(config)#
```

14.1.5 help

Standard ACL Config Commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-std-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-std-nacl)#
```

14.1.6 mark

Standard ACL Config Commands

Use this CLI command to specify packet that you want to mark.

Syntax

```
mark(8021.1p<0-7>|tos<0-255>)(A.B.C.D/M|any|host)

mark(8021.1p<0-7>|tos<0-255>)any|host(log|rule-precedence<1-5000>|
wlan<1-32>|A.B>C.D)

mark(8021.1p<0-7>|tos<0-255>)any wlan<1-32>(log|rule-precedence<1-5000>)
```

Parameters

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

14.1.7 no

Standard ACL Config Commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no(deny|mark|permit)
```

This command negates all the syntax combinatins that you have used in *deny*, *mark* and *permit* to configure the Extended ACL.

Parameters

deny	Specify packets to reject
mark	Specify packets to mark
permit	Specify packets to forward

Usage Guidelines

Example

14.1.8 permit

Standard ACL Config Commands

```
permit(A.B.C.D/M|any|host)
permit any(log|rule-precedence|wlan)
permit any log(rule-precedence)<1-500>
permit any rule-precedence<1-500>
permit any wlan<1-32>(log|rule-precedence)(rule-precedence)<1-500>
permit host A.B.C.D
```

Parameters

A.B.C.D/M	Source IP address range to match
any	Any source IP address
log	Log matches against this entry
rule-precedence*<1-500>*	Access-list entry precedence
<1-500>	Precedence Value
wlan*<1-32>*	Filter packets based on WLAN
<1-32>	WLAN index
host	Single host address
A.B.C.D	Exact source IP address to match

Usage Guidelines

Example

```
WS5100(config-std-nacl)#permit any log rule-precedence 50
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#permit any rule-precedence 60
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#permit any wlan 30 log rule-precedence 250
WS5100(config-std-nacl)#
```

14.1.9 service

Standard ACL Config Commands

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-if)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information.
diag-shell	Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Show running system information.
start-shell	Provide shell access.
tethereal	Dump and analyze network traffic.

Usage Guidelines

Example

```
WS5100(config-std-nacl)#service diag-shell
Diagnostic shell started for testing
diag >

WS5100(config-std-nacl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
WS5100(config-std-nacl)#
```

```
WS5100(config-std-nacl)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
WS5100(config-std-nacl)#service show

WS5100(config-std-nacl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp packet
only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]

WS5100(config-std-nacl)#
```

14.1.10 show

Standard ACL Config Commands

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show<paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

Example

```
WS5100(config-std-nacl)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
```

```
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-std-nacl)#show
```

14.1.11 terminal

Standard ACL Config Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults
monitor	Copy debug output to the current terminal line

Usage Guidelines

Example

```
WS5100(config-std-nacl)#terminal monitor
WS5100(config-std-nacl)#

WS5100(config-std-nacl)#terminal no monitor
WS5100(config-std-nacl)#
```

15

Extended MAC ACL Instance

Use **(config-ext-macl)** instance to configure the **mac access-list extended** ACLs associated with the WS5100 Series Wireless Switch.

15.1 MAC Extended ACL Config Commands

Table 15.1 summarizes the **config-ext-macl** commands within the WS5100 Series Switch command line

Table 15.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	page 15-3
deny	Specify packets to reject	page 15-4
end	End current mode and change to EXEC mode	page 15-6
exit	End current mode and down to previous mode	page 15-7

Command	Description	Ref.
help	Description of the interactive help system	page 15-8
mark	Specify packets to mark	page 15-9
no	Negate a command or set its defaults	page 15-11
permit	Specify packets to forward	page 15-12
service	Service Commands	page 15-13
show	Show running system information	page 15-15
terminal	Set terminal line parameters	page 15-17

15.1.1 clrscr

MAC Extended ACL Config Commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-macl)#clrscr
WS5100(config-ext-macl)#
```

15.1.2 deny

MAC Extended ACL Config Commands

Use this CLI command to specify packets that you want to reject.

Syntax

```
deny(Source MAC Address)(Destination MAC Address)
(dot1p<0-7>|type|vlan<1-4095>|wlan<1-32>)rule-precedende<1-5000>

deny(Source MAC Address)(Destination MAC Address)dot1p<0-7>
rule-precedence<1-5000>

deny(Source MAC Address)(Destination MAC Address)type
(<1-65535>|arp|ip|ipv6|vlan|wisp>)rule-precedence<1-5000>

deny(Source MAC Address)(Destination MAC Address)wlan<1-32>
(dot1p<0-7>|type|vlan<1-4095>)rule-precedence<1-5000>
```

Parameters

Source Mask	Source MAC Address can be one of the following: • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx– Source MAC address and mask • any – Any source host • host – Exact source MAC address to match
Destination Mask	Destination MAC Address can be one of the following • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx– Destination MAC address and mask • any – Any destination host • host – Exact destination MAC address to match
dot1p<*0-7*>	802.1p priority
rule-precedence<*1-5000*>	Access-list entry precedence
type(<*1-65535*>|arp|ip|ipv6|vlan|wisp)	EtherType
vlan<*1-4095*>	VLAN ID
wlan<*1-32*>	Filter packets based on WLAN

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

15.1.3 end

MAC Extended ACL Config Commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-macl)#end
WS5100#
```

15.1.4 exit

MAC Extended ACL Config Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-macl)#exit
WS5100(config)#
```

15.1.5 help

MAC Extended ACL Config Commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-ext-macl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-ext-macl)#
```

15.1.6 mark

MAC Extended ACL Config Commands

Use this CLI command to specify packet that you want to mark.

Syntax

```
mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
(dot1p<0-7>|type|vlan<1-4095>|wlan<1-32>)rule-precedence<1-5000>

mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
dot1p<0-7> rule-precedence<1-5000>

mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
type(<1-65535>|arp|ip|ipv6|vlan|wisp)rule-precedence<1-5000>

mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
vlan<1-4095> rule-precedence<1-5000>

mark(802.1p<0-7>|tos<0-255>)(Source MAC Address)(Destination MAC Address)
wlan<1-32>(dot1p<0-7>|type|vlan<1-4095>)rule-precedence<1-5000>
```

Parameters

8021p<*0-7*>	Modify 802.1p VLAN user priority
tos<*0-255*>	Modify TOS bits in IP header
Source MAC Address	Source MAC Address can be one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`– Source MAC address and mask • `any` – Any source host • `host` – Exact source MAC address to match
Destination MAC Address	Destination MAC Address can be one of the following • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`– Destination MAC address and mask • `any` – Any destination host • `host` – Exact destination MAC address to match
dot1p<*0-7*>	802.1p priority
rule-precedence<*1-5000*>	Access-list entry precedence

type(*<1-65535>*|arp|ip|ipv6|vlan|wisp)	EtherType
vlan*<1-4095>*	VLAN ID
wlan*<1-32>*	Filter packets based on WLAN

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

15.1.7 no

MAC Extended ACL Config Commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no(deny|mark|permit)
```

This command negates all the syntax combinatins that you have used in *deny*, *mark* and *permit* to configure the Extended ACL.

Parameters

deny	Specify packets to reject
mark	Specify packets to mark
permit	Specify packets to forward

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

15.1.8 permit

▶ *MAC Extended ACL Config Commands*

Use this CLI command to specify packets that you want to forward.

Syntax

```
permit(Source MAC Address)(Destination MAC Address)
(dot1p<0-7>|type|vlan<1-4095>|wlan<1-32>)rule-precedende<1-5000>

permit(Source MAC Address)(Destination MAC Address)dot1p<0-7>
rule-precedence<1-5000>

permit(Source MAC Address)(Destination MAC Address)type
(<1-65535>|arp|ip|ipv6|vlan|wisp>)rule-precedence<1-5000>

permit(Source MAC Address)(Destination MAC Address)wlan<1-32>
(dot1p<0-7>|type|vlan<1-4095>)rule-precedence<1-5000>
```

Parameters

Source MAC Address	Source MAC Address can be one of the following: • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx– Source MAC address and mask • any – Any source host • host – Exact source MAC address to match
Destination MAC Address	Destination MAC Address can be one of the following • xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx– Destination MAC address and mask • any – Any destination host • host – Exact destination MAC address to match
dot1p<*0-7*>	802.1p priority
rule-precedence<*1-5000*>	Access-list entry precedence
type(<*1-65535*>|arp|ip|ipv6|vlan|wisp)	EtherType
vlan<*1-4095*>	VLAN ID
wlan<*1-32*>	Filter packets based on WLAN

15.1.9 service

MAC Extended ACL Config Commands

SyntaxUse this CLI command to invoke the service commands to trobuleshoot or debug the `(config-if)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Remove specified support information.
diag-shell	Provide diagnostic shell access to debug and test the WS5100 Series Wireless Switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Show running system information.
start-shell	Provide shell access.
tethereal	Dump and analyze network traffic.

Usage Guidelines

Example

```
WS5100(config-ext-macl)#service diag-shell
Diagnostic shell started for testing
diag >
  boot            Reboots the switch
  delete          Deletes specified file from the system.
  exit            Exit from the CLI
  fallback        Configures firmware fallback feature
  help            Description of the interactive help system
  logout          Exit from the CLI
  no              Negate a command or set its defaults
  reload          Halt and perform a warm reboot
  service         Service Commands
  show            Show running system information
  upgrade         Upgrade firmware image
diag >
```

```
WS5100(config-ext-macl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
WS5100(config-ext-macl)#

WS5100(config-ext-macl)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
WS5100(config-ext-macl)#service show

WS5100(config-ext-macl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
WS5100(config-ext-macl)#

WS5100(config-ext-macl)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp packet
only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]
WS5100(config-ext-macl)#service tethereal
```

15.1.10 show

MAC Extended ACL Config Commands

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show<paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

Example

```
WS5100(config-ext-macl)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
```

```
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-ext-macl)#show
```

15.1.11 terminal

MAC Extended ACL Config Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults
monitor	Copy debug output to the current terminal line

Usage Guidelines

Example

```
WS5100(config-ext-macl)#terminal monitor
WS5100(config-ext-macl)#

WS5100(config-ext-macl)#terminal no monitor
WS5100(config-ext-macl)#
```

16

Radius Server Instance

The **`radius-server local`** cli command takes you to radius server mode.The local (Onboard) radius server configuration commands are listed under this mode. Use **`(config-radsrv)`**instance to configure local radius server parameters associated with the WS5100 Series Wireless Switch.

16.1 Radius Configuration Commands

Table 16.1 summarizes the Gloabl Config commands within the WS5100 Series Switch command line

Table 16.1 Extended ACL Config Command Summary

Command	Description	Ref.
authentication	Radius authentication	page 16-3
ca	Configure ca certificate parameters	page 16-4
clrscr	Clears the display screen	page 16-5
crl-check	Certificate Revocation List(CRL) check	page 16-6

Command	Description	Ref.
end	End current mode and change to EXEC mode	page 16-7
exit	End current mode and down to previous mode	page 16-8
group	Configure radius user group paramaters. **NOTE** This command create another sub-instance called **`config-radsrv-group`** with its own set of command summary.	page 16-9
help	Description of the interactive help system	page 16-21
ldap-server	ldap server parameters	page 16-22
nas	Radius client	page 16-23
no	Negate a command or set its defaults	page 16-24
proxy	Radius proxy server	page 16-25
rad-user	Radius user configuration	page 16-27
server	Configure server certificate parameters	page 16-28
service	Service Commands	page 16-29
show	Show running system information	page 16-30
terminal	Set terminal line parameters	page 16-32

16.1.1 authentication

Radius Configuration Commands

<<< Text here>>>

Syntax

```
authentication(data-source|eap-auth-type)
authentication data-source(ldap|local)
authentication eap-auth-type(all|peap-gtc|peap-mschapv2|tls|ttls-md5|
ttls-mschapv2|ttls-pap)
```

Parameters

data-source	Radius Datasource for user authentication
eap-auth-type	Radius Eap and Default authentication type configuration
all	Enable both ttls and peap
peap-gtc	Eap type peap with Default auth type gtc
peap-mschapv2	Eap type peap with Default auth type mschapv2
tls	Eap type tls
ttls-md5	EAP type ttls with Default auth type md5
ttls-mschapv2	EAP type ttls with Default auth type mschapv2
ttls-pap	EAP type ttls with Default auth type pap

Usage Guidelines

Example

16.1.2 ca

Radius Configuration Commands

Use this CLI command to configure CA (Certificate Authority) parameters.

Syntax

```
ca trust-point(WORD)
```

Parameters

trust-point	Trust point configuration
WORD	Existing trust point name

Usage Guidelines

Configure the trustpoint that is used by the local radius server.Ensure you create the **`trustpoint`** before it is used by the **`Crypto pki trustpoint`** command.

Example

16.1.3 clrscr

Radius Configuration Commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-radsrv)#clrscr
WS5100(config-radsrv)#
```

16.1.4 crl-check

Radius Configuration Commands

Use this CLI command to enable Certificate Revocation List(CRL) check.To enable the certificate revocation list ensure the `crl list` is loaded using **`crypto pki import <trustpoint-name> crl`** command.

Syntax

```
crl-check
```

Parameters

enable	enable CRL check

Usage Guidelines

Example

```
WS5100(config-radsrv)#crl-check enable
WS5100(config-radsrv)#
```

16.1.5 end

Radius Configuration Commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-radsrv)#end
WS5100#
```

16.1.6 exit

Radius Configuration Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-radsrv)#exit
WS5100(config)#
```

16.1.7 group

Radius Configuration Commands

Use this CLI command to configure radius user group paramaters.The system moves to a sub-instance mode when you create a new group and the prompt changes from **`WS5100(config-radsrv)#`** to **`WS5100(config-radsrv-group)#.`**

Table 16.2 summarizes the Radius User Group commands withing the (config-radsrv-group) sub-instance.

Table 16.2 Radius User Group Configuration Command Summary

Command	Description	Ref.
clrscr	Clears the display screen	
end	End current mode and change to EXEC mode	
exit	End current mode and down to previous mode	
group	Configure radius user group paramaters	
guest-group	Guest group configuration	
help	Description of the interactive help system	
no	Negate a command or set its defaults	
policy	Radius group access policy configuration	
rad-user	Add Radius user to this group	
service	Service Commands	
show	Show running system information	
terminal	Set terminal line parameters	

16.1.7.1 clrscr

Radius Configuration Commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
WS5100(config-radsrv-group)#clrscr
WS5100(config-radsrv-group)#
```

16.1.7.2 end

Radius Configuration Commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

```
end
```

Parameters

None.

Example

```
WS5100(config-radsrv-group)#end
WS5100#
```

16.1.7.3 exit

Radius Configuration Commands

Use this CLI command to end current mode and down to previous mode (`config-radsrv`)). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
WS5100(config-radsrv-group)#exit
WS5100(config-radsrv)#group
```

16.1.7.4 group

Radius Configuration Commands

Use this CLI command to configure radius user group paramaters.

Syntax

```
group
```

Parameters

WORD	Radius group name

Example

```
WS5100(config-radsrv-group)#group TestGroup
WS5100(config-radsrv-group)#
```

16.1.7.5 guest-group

Radius Configuration Commands

Use this CLI command to configure a guest group.

Syntax

```
guest-group
```

Parameters

enable	Enable this group as guest group

Example

```
WS5100(config-radsrv-group)#guest-group enable
WS5100(config-radsrv-group)#
```

16.1.7.6 help

Radius Configuration Commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
WS5100(config-radsrv-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-radsrv-group)#
```

16.1.7.7 no

Radius Configuration Commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no(policy|rad-user|service)
no policy(day|time|vlan|wlan)
no policy wlan(<1-32>|all)<1-32>
```

Parameters

policy	Radius group access policy configuration
day	Reset day of access policy for this group
time	Configure time of access policy for this group
vlan	VLAN id for this group
wlan	Configure wlan access policy for this group
<1-32>	Wlan Range
all	Remove all the wlan's allowed
rad-user	Remove user from this group
WORD	Existing user name in this group
all	Remove all users from this group
service	Service Commands
radius	Disable radius server

Example

```
WS5100(config-radsrv-group)#no policy day
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no policy time
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no policy vlan
WS5100(config-radsrv-group)#
```

```
WS5100(config-radsrv-group)#no policy wlan 2 5
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no rad-user all
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#no service radius
%%Info: Radius service stopped...
WS5100(config-radsrv-group)#
```

16.1.7.8 policy

Radius Configuration Commands

Use this CLI command to configure Radius group access policy.

Syntax

```
policy(day|time|vlan|wlan)
policy day(all|fr|mo|sa|su|th|tu|we|weekdays)
ploicy time(start|end)<0-23><0-59>
policy vlan<1-4094>
```

Parameters

day	Day of access policy configuration
all	All days (from Sunday to Saturday)
fr	Friday
mo	Monday
sa	Saturday
su	Sunday
th	Thursday
tu	Tuesday
we	Wednesday
weekdays	Allow access only in week days (Mo-Fr)
time	Configure time of access policy for this group
start	Start time
end	End Time must be greater than the start time

<0-23>	hour (hh) limit
<0-59>	mins (mm) limit
vlan	VLAN id for this group
<1-4094>	VLAN range
wlan	Configure wlan access policy for this group
<1-32>	Wlan index

Example

```
WS5100(config-radsrv-group)#policy day weekdays
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#policy time start 12 12 end 22 22
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#policy vlan 20
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#policy wlan 20 21 22 23
WS5100(config-radsrv-group)#
```

16.1.7.9 rad-user

▶ *Radius Configuration Commands*

Use thie CLI command to add Radius user to this group.

Syntax

```
rad-user
```

Parameters

WORD	Existing radius user name

Example

16.1.7.10 service

Radius Configuration Commands

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-radsrv-group)` instance configurations.This command is also used to enable RADIUS server.

Syntax

```
service(clear|diag-shell|radius|save-cli|show|start-shell|tethereal)
service radius restart
```

Parameters

clear	Remove specified support information
diag-shell	Provide diag shell access
radius	Enable radius server restart
save-cli	Save CLI tree for all modes in html format
show	Show running system information
start-shell	Provide shell access
tethereal	Dump and analyze network traffic

Example

```
WS5100(config-radsrv-group)#service radius restart
WS5100(config-radsrv-group)#
```

16.1.7.11 show

Radius Configuration Commands

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show<paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-radsrv-group)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-radsrv-group)#
```

16.1.7.12 terminal

Radius Configuration Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults
monitor	Copy debug output to the current terminal line

Usage Guidelines

Example

```
WS5100(config-radsrv-group)#terminal monitor
WS5100(config-radsrv-group)#

WS5100(config-radsrv-group)#terminal no monitor
WS5100(config-radsrv-group)#
```

16.1.7.13 Example–Creating a Group

The usage of **(config-radsrv-group)** sub-instance is explained through an example illustrated below:

1. Create a group called **Sales** in the local radius server database.
   WS5100(config-radsrv)#group sales
2. Check the Radius user group configuration commands.
   WS5100(config-radsrv-group)#?

```
Radius user group configuration commands:
  clrscr       Clears the display screen
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  group        Configure radius user group paramaters
  guest-group  Guest group configuration
  help         Description of the interactive help system
  no           Negate a command or set its defaults
  policy       Radius group access policy configuration
  rad-user     Add Radius user to this group
  service      Service Commands
  show        Show running system information
```

3. Use **policy** command to configure the group policies for the group created in Step 1.
   WS5100(config-radsrv-group)#policy ?

```
day   Day of access policy configuration
time  Configure time of access policy for this group
vlan  VLAN id for this group
wlan  Configure wlan access policy for this group

WS5100(config-radsrv-group)#policy day weekdays
WS5100(config-radsrv-group)#policy time start 12 30 end 15 30
```

4. Use **policy vlan** command to assign an vlan id of 10 to group Sales
   `WS5100(config-radsrv-group)#policy vlan 10`
5. Use **policy wlan** command to allow only authorised users to access this groups wlan
   `WS5100(config-radsrv-group)#policy wlan 1 2 5`

6. Use `(config-radsrv)#rad-user` to create a user called **testuser** and add it to group **Sales**

```
WS5100(config-radsrv)#rad-user testuser password testpassword group sales
Sep 08 17:41:55 2006: RADCONF: Adding user "testuser" into local database
Sep 08 17:41:55 2006: RADCONF: User "testuser" is added to group "sales"
```

7. Use `(config-radsrv)#nas` to add a NAS entry for the group

```
WS5100(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

WS5100(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

WS5100(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

WS5100(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

8. Use `(config-radsrv)#proxy` to add a realm name for the group.

```
WS5100(config-radsrv)#proxy realm mydomain.com server 10.10.1.10 port 1812
secret 0 testing
```

9. Save the changes and restart the radius service.

```
WS5100(config-radsrv)#service radius restart
Sep 08 17:48:04 2006: %PM-5-PROCSTOP: Process "radiusd" has been stopped
Sep 08 17:48:05 2006: RADCONF: radius config files generated successfully
WS5100(config-radsrv)#Sep 08 17:48:05 2006: %DAEMON-6-INFO: radiusd[8830]:
Ready to process requests.
```

16.1.8 help

Radius Configuration Commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-radsrv)#help?
  help  Description of the interactive help system

WS5100(config-radsrv)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-radsrv)#
```

16.1.9 ldap-server

Radius Configuration Commands

Use thie CLI command to configure LDAP server parameters.

Syntax

```
ldap-server(primary|secondary)host(A.B.C.D)
```

Parameters

primary	primary ldap server configuration
secondary	secondary ldap server configuration
host	ldap server ip configuration
A.B.C.D	ldap server ip address

Usage Guidelines

Example

16.1.10 nas

Radius Configuration Commands

Use this CLI to configure the RADIUS client.

Syntax

`nas(A.B.C.D/M)key(0|2|LINE)`

Parameters

A.B.C.D/M	Radius Client IP address
key	Radius Client shared key
0	Password is specified UNENCRYPTED
2	Password is encrypted with password-encryption secret
LINE	The secret (client shared secret),upto 32 characters.

Example

```
WS5100(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

WS5100(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

WS5100(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

WS5100(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

16.1.11 no

Radius Configuration Commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no(authentication|ca|crl-check|group|ldap-server|nas|proxy|rad-
user|server|service)
```

Parameters

authentication	Radius authentication
ca	Configure ca certificate parameters
crl-check	Certificate Revocation List(CRL) check
group	Local radius server group configuration
ldap-server	ldap server parameters
nas	Radius client
proxy	Radius proxy server
rad-user	Radius user configuration
server	Configure server certificate parameters
service	Service Commands

Usage Guidelines

Example

```
WS5100(config-radsrv)#no authentication data-source
WS5100(config-radsrv)#

WS5100(config-radsrv)#no ca trust-point
WS5100(config-radsrv)#
```

16.1.12 proxy

Radius Configuration Commands

Use this CLI command to configure RADIUS proxy server.

Syntax

```
proxy(realm|retry-count|retry-delay)
proxy relam(WORD)server(A.B.C.D)port(<1024-65535>)secret(0|2|WORD)
```

Parameters

realm WORD	Realm name
WORD	A string of up to 50 characters
server (A.B.C.D)	proxy server
A.B.C.D	proxy server ip address
port <1024-65535>	proxy server port
<1024-65535>	proxy server port number
secret *(0|2|WORD)*	proxy server secret string
0	Password is specified UNENCRYPTED
2	Password is encrypted with password-encryption secret
WORD	the proxy server shared secret upto 32 characters
retry-count *<3-6>*	Proxy server retry count value
<3-6>	Retry count (in numbers)
retry-delay*<5-10>*	Proxy server retry delay time
<5-10>	retry delay time (in seconds)

Usage Guidelines

Example

```
WS5100(config-radsrv)#proxy realm Test server 10.10.10.1 port 2220 secret
"Very Very Secret !!!"
WS5100(config-radsrv)#

WS5100(config-radsrv)#proxy retry-count 5
WS5100(config-radsrv)#

WS5100(config-radsrv)#proxy retry-delay 8
WS5100(config-radsrv)#
```

16.1.13 rad-user

Radius Configuration Commands

Use this CLI to configure RADIUS user parameters.

Syntax

```
rad-user(WORD)password(0|2|WORD)
```

Parameters

WORD	Enter user name upto 64 characters length
password(0|2|WORD)	Radius user password
0	Password is specified UNENCRYPTED
2	Password is encrypted with password-encryption secret
WORD	Enter password upto 21 characters length

Usage Guidelines

Example

```
WS5100(config-radsrv)#rad-user TestRadUser password "I SPY U"
WS5100(config-radsrv)#
```

16.1.14 server

Radius Configuration Commands

Use this CLI command to configure server certificate parameters. You must create a trustpoint using `crypto-pki-trustpoint` or have an existing trustpoint to configure `server`.

Syntax

```
server trust-point
```

Parameters

trust-point	Trust point configuration
WORD	Existing trust point name

Usage Guidelines

Example

```
WS5100(config-radsrv)#server trust-point TestTP
%%Error: Specified Trust-point does not exists
WS5100(config-radsrv)#
```

16.1.15 service

Radius Configuration Commands

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-radsrv)` instance configurations.This command is also used to enable RADIUS server.

Syntax

```
service(clear|diag-shell|radius|save-cli|show|start-shell|tethereal)
service radius restart
```

Parameters

clear	Remove specified support information
diag-shell	Provide diag shell access
radius	Enable radius server restart
save-cli	Save CLI tree for all modes in html format
show	Show running system information
start-shell	Provide shell access
tethereal	Dump and analyze network traffic

Example

```
WS5100(config-radsrv-group)#service radius restart
WS5100(config-radsrv-group)#
```

16.1.16 show

Radius Configuration Commands

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show<paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Example

```
WS5100(config-radsrv)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
```

```
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  startup-config        Contents of startup configuration
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

WS5100(config-radsrv)#show
```

16.1.17 terminal

Radius Configuration Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults
monitor	Copy debug output to the current terminal line

Usage Guidelines

Example

```
WS5100(config-radsrv)#terminal monitor
WS5100(config-radsrv)#

WS5100(config-radsrv)#terminal no monitor
WS5100(config-radsrv)#
```

17

Wireless Instance

Use **`(config-wireless)`**instance to configure local radius server parameters associated with the WS5100 Series Wireless Switch.

17.1 Wireless Configuration Commands

Table 17.1 summarizes the Gloabl Config commands within the WS5100 Series Switch command line

Table 17.1 Extended ACL Config Command Summary

Command	Description	Ref.
adopt-unconf-radio	Adopt a radio even if its not yet configured. The default templates will be used for configuration.	page 17-4
adoption-pref-id	A preference identifier for this wireless switch. All radios configured with this preference identifier are more likely to be adopted by this wireless-switch	page 17-5
ap-detection	AP detection configuration commands	page 17-6

Command	Description	Ref.
broadcast-tx-speed	Set the rate at which broadcast and multicast traffic should be transmitted	page 17-8
clrscr	Clears the display screen	page 17-9
convert-ap	Change the mode of operation of an AP	page 17-10
country-code	Configure the country of operation. All existing radio configuration will be erased	page 17-11
dhcp-sniff-state	Record mobile-unit DHCP state information	page 17-14
dot11-shared-key-auth	Enable support for 802.11 shared key authentication.	page 17-15
end	End current mode and change to EXEC mode	page 17-16
exit	End current mode and down to previous mode	page 17-17
fix-windows-dhcp	Convert Windows DHCP server responses to be Unicast instead of Broadcast	page 17-18
help	Description of the interactive help system	page 17-19
ids	Intrusion Detection configuration commands	page 17-20
mac-auth-local	local mac authentication list	page 17-22
manual-wlan-mapping	Allow manual mapping/un-mapping of wlans to configured radios	page 17-23
mobility	Configure Mobility parameters	page 17-24
no	Negate a command or set its defaults	page 17-25
oversized-frames	Attempt to use oversized frames for data traffic	page 17-26
proxy-arp	Respond to ARP requests from the RON to WLAN on behalf of mobile-units	page 17-27
qos-mapping	QoS mappings between the wired and wireless domains	page 17-28
radio	Radio related commands	page 17-29
self-heal	Self Healing configuration commands	page 17-36

Command	Description	Ref.
sensor	Wireless Intrusion Protection System parameters	page 17-38
service	Service Commands	page 17-39
show	Show running system information	page 17-42
smart-scan-channels	Specify a list of channels that are used on the network. This list will be provided to mobile-units that can support partial scanning	page 17-44
terminal	Set terminal line parameters	page 17-45
wlan	Wireless LAN related commands	page 17-46

17.1.1 adopt-unconf-radio

Wireless Configuration Commands

Use this CLI command to adopt a radio even if its not yet configured. The default templates will be used for configuration.

Syntax

```
adopt-unconf-radio
```

Parameters

enable	Enable the adoption of unconfigured radios

Usage Guidelines

Example

```
WS5100(config-wireless)#adopt-unconf-radio enable
WS5100(config-wireless)#
```

17.1.2 adoption-pref-id

Wireless Configuration Commands

Use this CLI command as a preference identifier for the WS5100 wireless switch. All radios configured with this preference identifier are more likely to be adopted by this wireless-switch.

Syntax

```
adoption-pref-id
```

Parameters

<1-65535>	Select a Pref-ID within 1-65535.

Usage Guidelines

Example

```
WS5100(config-wireless)#adoption-pref-id 500
WS5100(config-wireless)#
```

17.1.3 ap-detection

Wireless Configuration Commands

Use this CLI command to configure AP detection.

Syntax

```
ap-detection(approved|enable|max-aps|mu-assisted-scan|timeout)
ap-detection approved add <1-200> (MAC Address)(SSID)
ap-detection mu-assisted-scan(enable|refresh<10-86400>)
```

Parameters

approved	The approved AP list
add	Add an entry to the approved AP list.
<1-200>	Index where this approved entry will be added: <1-200>
MAC Address	You can select either: • MAC–Mac address in AA-BB-CC-DD-EE-FF format • any–any Mac address
SSID	You can select either: • LINE–A string of up to 32 characters • any–any ssid
enable	Allow access-ports to look for APs
max-aps*<1-1000>*	Select the maximum amount of entries for unapproved-seen and approved-seen that can showed.
mu-assisted-scan	mobile-unit assisted scanning
enable	enable mobile-unit assisted scanning
refresh*<10-86400>*	The period in seconds with which all scan-capable mobile-units are requested to scan for neighboring APs.
timeout *<1-65535>*	The amount of seconds a AP will remain in the list after it is no longer seen

Usage Guidelines

Example

```
WS5100(config-wireless)#ap-detection enable
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection approved add 150 any any
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection max-aps 250
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection mu-assisted-scan enable
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection mu-assisted-scan refresh 520
WS5100(config-wireless)#

WS5100(config-wireless)#ap-detection timeout 500
WS5100(config-wireless)#
```

17.1.4 broadcast-tx-speed

Wireless Configuration Commands

Use this CLI command to configure the rate at which broadcast and multicast traffic should be transmitted between the WS5100 wireless switch and MU's.

Syntax

```
broadcast-tx-speed(range|throughput)
```

Parameters

range	use lowest basic rate. Provides maximum range
throughput	use highest basic rate. Provides maximum throughput (default)

Usage Guidelines

Example

```
WS5100(config-wireless)#broadcast-tx-speed range
WS5100(config-wireless)#

WS5100(config-wireless)#broadcast-tx-speed throughput
WS5100(config-wireless)#
```

17.1.5 clrscr

Wireless Configuration Commands

Use this CLI command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-wireless)#clrscr
WS5100(config-wireless)#
```

17.1.6 convert-ap

Wireless Configuration Commands

Use this CLI command to change the mode of operation of an AP to either sensor or standalone.

Syntax

```
convert-ap <1-48>(default|sensor|standalone)
```

Parameters

<1-48>	Indices of the APs to be converted, from the ['show wireless ap' command]
default	do not force any conversion. Let the AP negotiate its normal mode of operation with the switch.
sensor	Convert an AP300 to operate as an IDS sensor. **NOTE** The switch will not be able to adopt this AP again until it is converted back to a regular AP300 using the [sensor MAC revert-to-ap] command
standalone	Convert a thin AP4131 back to a stand-alone AP. **NOTE** The switch will not be able to adopt this AP again until the AP is converted back to a thin-AP using the APs configuration interface

Usage Guidelines

Example

17.1.7 country-code

Wireless Configuration Commands

USe this CLI command to configure the country of operation. All existing radio configuration will be erased when u use this command.

Syntax

```
country-code
```

Parameters

Abbrevation	Use the country abbrevation to confiugre the WS5100 switch to operate in a particular country.

Usage Guidelines

Example

```
WS5100(config-wireless)#country-code ?
  ae  United Arab Emirates
  ar  Argentina
  at  Austria
  au  Australia
  ba  Bosnia Herzegovina
  be  Belgium
  bg  Bulgaria
  bh  Bahrain
  bm  Bermuda
  br  Brazil
  bs  Bahamas
  by  Belarus
  ca  Canada
  ch  Switzerland
  cl  Chile
  cn  China
  co  Colombia
  cr  Costa Rica
  cy  Cyprus
  cz  Czech Republic
  de  Germany
  dk  Denmark
  do  Dominican Republic
  ec  Ecuador
  ee  Estonia
  eg  Egypt
  es  Spain
```

```
fi  Finland
fr  France
gb  United Kingdom
gr  Greece
gt  Guatemala
gu  Guam
hk  Hong Kong
hn  Honduras
hr  Croatia
ht  Haiti
hu  Hungary
id  Indonesia
ie  Ireland
il  Israel
in  India
is  Iceland
it  Italy
jo  Jordan
jp  Japan
kr  South Korea
kw  Kuwait
kz  Kazakhstan
li  Liechtenstein
lk  Sri Lanka
lt  Lithuania
lu  Luxembourg
lv  Latvia
ma  Morocco
mt  Malta
mx  Mexico
my  Malaysia
nl  Netherlands
no  Norway
nz  New Zealand
om  Oman
pe  Peru
ph  Philippines
pk  Pakistan
pl  Poland
pt  Portugal
qa  Qatar
ro  Romania
ru  Russia
sa  Saudi Arabia
se  Sweden
sg  Singapore
si  Slovenia
sk  Slovak Republic
th  Thailand
```

```
  tr  Turkey
  tw  Taiwan
  ua  Ukraine
  us  United States
  uy  Uruguay
  ve  Venezuela
  vn  Vietnam
  za  South Africa

WS5100(config-wireless)#country-code
```

17.1.8 dhcp-sniff-state

Wireless Configuration Commands

Use this CLI ccommand to record mobile-unit DHCP state information.

Syntax

```
dhcp-sniff-state
```

Parameters

enable	Enable support for recording DHCP state information for mobile-units.

Usage Guidelines

Example

```
WS5100(config-wireless)#dhcp-sniff-state enable
WS5100(config-wireless)#
```

17.1.9 dot11-shared-key-auth

Wireless Configuration Commands

Use this CLI command to Enable support for 802.11 shared key authentication.

NOTE Shared key authentication has known weaknesses that can compromise your WEP key. It should only be configured to accomodate wireless stations that are unable to carry out Open-System authentication.

Syntax

```
dot11-shared-key-auth
```

Parameters

enable	Enable support for shared key authentication.

Usage Guidelines

Example

```
WS5100(config-wireless)#dot11-shared-key-auth enable
WS5100(config-wireless)#
```

17.1.10 end

Wireless Configuration Commands

Use this CLI command to endand exit from the current mode and change to PRIV EXEC mode.The prompt now changes to `WS5100#`.

Syntax

end

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-wireless)#end
WS5100#
```

17.1.11 exit

Wireless Configuration Commands

Use this CLI command to end current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `WS5100(config)#`.

Syntax

```
exit
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-wireless)#exit
WS5100(config)#
```

17.1.12 fix-windows-dhcp

Wireless Configuration Commands

Use this CLI command to convert Windows DHCP server responses to be Unicast instead of Broadcast

Syntax

```
fix-windows-dhcp
```

Parameters

enable	Enable support for converting Windows DHCP server responses

Usage Guidelines

Example

```
WS5100(config-wireless)#fix-windows-dhcp enable
WS5100(config-wireless)#
```

17.1.13 help

Wireless Configuration Commands

Use thie CLI command to access the systems interactive help system.

Syntax

```
help
```

Parameters

None.

Usage Guidelines

Example

```
WS5100(config-wireless)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

WS5100(config-wireless)#
```

17.1.14 ids

Wireless Configuration Commands

Use this CLI command to configure Intrusion Detection System.

Syntax

```
ids(anomaly-detection|detect-window|ex-ops)

ids anomaly-detection(all|invalid-frame-length|multicast-source|
null-destination|same-source-destination|tkip-countermeasures|weak-wep-iv)
(enable|filter-ageout)

ids detect-window<5-300>

ids ex-ops(80211-replay-fails|all|association-requests|
authentication-fails|crypto-replay-fails|decryption-fails|
disassociations|eap-starts|probe-requests|unassoc-frames)
(filter-ageout<0-86400>|threshold(mu|radio|switch)<0-9999>)
```

Parameters

anomaly-detection	Configure parameters related to the detection of anomalous frames on the RF network.
all	Enable for all types of anomalous frames
invalid-frame-length	invalid frame lengths
multicast-source	broadcast or multicast source
null-destination	all zero's addess
same-source-destination	identical source and destination addresses
tkip-countermeasures	filter mobile units that cause tkip countermeasures
weak-wep-iv	use of weak wep sequence numbers
enable	Enable monitoring and filtering
filter-ageout	Set the number of seconds for which mobile units will be filtered out.
detect-window*<5-300>*	Set the number of seconds for which information will be collected before analysis. All the thresholds are a function of this window size.
ex-ops	Configure parameters related to the detection of excessive operations on the RF network.

80211-replay-fails	802.11 replay check failure
all	Change for all types of excessive operations
association-requests	802.11 Authentication and Association Requests
authentication-fails	Failure to Authenticate with servers (Radius/Kerberos)
crypto-replay-fails	TKIP/CCMP IV replay check failure
decryption-fails	decryption failures
disassociations	Disassociation and Deauthentication frames
eap-starts	EAP (802.1x) Start frames
probe-requests	Probe Request frames
unassoc-frames	frames from unassociated stations
filter-ageout<0-86400>	Configure the number of seconds for which mobile units will be filtered out
threshold (*mu*|*radio*|*switch*)	Configure the threshold of events allowed in the detection window. • mu–Use the threshold for monitoring on a per-mobile-unit basis. • radio–Use the threshold for monitoring on a per-radio basis. • switch–Use the threshold for monitoring at the switch level.
<0-9999>	The threshold of events allowed in the detection window

Usage Guidelines

Example

```
WS5100(config-wireless)*#ids anomaly-detection tkip-countermeasures enable
WS5100(config-wireless)*#

WS5100(config-wireless)#ids detect-window 250
WS5100(config-wireless)#

WS5100(config-wireless)#ids ex-ops 80211-replay-fails filter-ageout 5200
WS5100(config-wireless)#
```

17.1.15 mac-auth-local

Wireless Configuration Commands

Use this CLI command to configure local MAC authentication list.

Syntax

```
mac-auth-local<1-1000> (allow|deny)(Starting MAC Address)(Ending MAC
Address)(range/list of WLAN indicies)WORD
```

Parameters

<1-1000>	mac-auth-local entry
allow	allow mobile-units that match this rule to associate
deny	deny association to mobile-units that match this rule
Starting MAC Address	Starting mac address in AA-BB-CC-DD-EE-FF format
Ending MAC Address	Ending mac address in AA-BB-CC-DD-EE-FF format
Range/List of WLAN Indices	A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices
WORD	Optional radio description substring

Usage Guidelines

Example

```
WS5100(config-wireless)#mac-auth-local 452 allow 12.11.11.120 12.11.11.150
3-7 TestString
WS5100(config-wireless)#
```

17.1.16 manual-wlan-mapping

Wireless Configuration Commands

Use this CLI command to manually map map/un-map the wlans configured on a radio.

Syntax

```
manual-wlan-mapping
```

Parameters

enable	Enable support for manual-wlan-mapping

Usage Guidelines

Example

```
WS5100(config-wireless)#manual-wlan-mapping enable
WS5100(config-wireless)#
```

17.1.17 mobility

Wireless Configuration Commands

Use this CLI command to configure mobility parameters

Syntax

```
mobility(enable|local-address|max-roam-period|peer)
mobility local-address (IP Address)
mobility max-roam-period<1-15>
mobililty peer (IP Address)
```

Parameters

enable	Enable Mobility Globally
local-address	Set Local Addr for Mobility
A.B.C.D	IP Address of A.B.C.D format
max-roam-period*<1-15>*	Set Max Roam Period for an MU (in seconds)
peer	Add a Peer to this mobility region
A.B.C.D	IP address of the Peer

Usage Guidelines

Example

```
WS5100(config-wireless)#mobility enable
WS5100(config-wireless)#

WS5100(config-wireless)#mobility local-address 12.12.12.1
WS5100(config-wireless)#

WS5100(config-wireless)#mobility max-roam-period 10
WS5100(config-wireless)#

WS5100(config-wireless)#mobility peer 157.208.235.108
WS5100(config-wireless)#
```

17.1.18 no

Wireless Configuration Commands

Use this CLI command to negate a command or set its defaults.

Syntax

```
no(adopt-unconf-radio|adoption-pref-id|ap-detection|broadcast-tx-
speed|country-code|dhcp-sniff-state|dot11-shared-key-auth|fix-windows-
dhcp|ids|mac-auth-local|manual-wlan-mapping|mobile-
unit|mobility|oversized-frames|proxy-arp|qos-mapping|radio|self-
heal|sensor|service|smart-scan-channels|wlan)
```

Parameters

Refer to *Table 17.1 on page 17-1* for the parameters that can be negated using **no** command.

Usage Guidelines

Example

```
WS5100(config-wireless)#no mobility enable
WS5100(config-wireless)#
```

17.1.19 oversized-frames

Wireless Configuration Commands

Use this CLI command to use oversized frames for data traffic.

Syntax

```
oversized-frames
```

Parameters

enable	Enable support for oversized frames

Usage Guidelines

Example

```
WS5100(config-wireless)#oversized-frames enable
WS5100(config-wireless)#
```

17.1.20 proxy-arp

Wireless Configuration Commands

Use thie CLI command respond to ARP requests from the RON to WLAN on behalf of mobile-units.

Syntax

```
proxy-arp
```

Parameters

enable	Enable support for proxy arp

Usage Guidelines

Example

```
WS5100(config-wireless)#proxy-arp enable
WS5100(config-wireless)#
```

17.1.21 qos-mapping

Wireless Configuration Commands

Use this CLI command to confiure and setup QoS mappings between the wired and wireless domains.

Syntax

```
qos-mapping(wired-to-wireless|wireless-to-wired)

qos-mapping wired-to-wireless(dot1p<0-7>|dscp<0-63>)
(background|best-effort|video|voice)

qos-mapping wireless-to-wired(background|best-effort|video|voice)
dot1p<0-7>
```

Parameters

wired-to-wireless	Mappings used while switching wired traffic over the air.
dot1p<*0-7*>	Configure mappings of 802.1p tags to access categories. You can specify more than one 802.1p tag (0-7) to be configured.
dscp<*0-63*>	Configure mappings of DSCP values to access categories. You can specify more than one DSCP value (0-63) to be configured.
background	background category traffic.
best-effort	best effort category traffic.
video	video traffic category traffic.
voice	voice traffic category traffic.
wireless-to-wired	Mappings used while switching wireless traffic to the RON side.
dot1p<*0-7*>	Configure the 802.1p tags that corresponds to selected access category.

Usage Guidelines

Example

```
WS5100(config-wireless)#qos-mapping wireless-to-wired background dot1p 5
WS5100(config-wireless)#
```

17.1.22 radio

Wireless Configuration Commands

Use thie CLI command to configure radio related settings.

Syntax

```
radio (<1-1000>|RADIO|add|all-11a|all-11b|all-11bg|
configure-8021X|default-11a|default-11b|default-11bg|dns-name)

radio<1-1000>(adoption-pref-id|antenna-mode|beacon-interval|bss|
cca-level|cca-mode|channel-power|coordinates|
copy-config-from|description|detector|dtim-period|enforce-spec-mgmt|
image-name|location-message|mac|max-mobile-units|
on-channel-scan|reset|reset-ap|rts-threshold|run-acs|
self-heal-offset|short-preamble|speed|wmm|)

radio bss(<1-4>|auto>)WLAN
radio channel-power(indoor|outdoor)(<1-200>|acs|random)<4-20>
radio coordinates (x coordinates) (y coordinates)(z coordinates)
radio copy-config-from(<1-1000>|default-11a|default-11b|default-11bg)
radio dtim-period<1-50> bss<1-4>
radio range(1|11|12|18|2|24|36|48|54|5p5|6|9|basic1|basic11basic12|
basic18|basic2|basic24|basic36|basic48|basic54|basic5p5|basic6|basic9|
default|range|throughput)
radio wmm(background|best-effort|video|voice)(aifsn<1-15>|burst<0-65535>|
cw<0-15>)
radio add<1-1000>(MAC Address)(11a(ap300)|11b(ap100|ap4131)|11bg(ap300))
```

Parameters

<1-1000>	A single radio index.
RADIO	A list (eg: 1,3,7) or range (eg: 3-7) of radio indices.
all-11a	all 11a radios currently in configuration.
all-11b	all 11b radios currently in configuration.
all-11bg	all 11bg radios currently in configuration.
configure-8021X	Configure 802.1X username and password on adopted access-ports.
default-11a	default 11a configuration template.
default-11b	default 11b configuration template.
default-11bg	default 11bg configuration template.

adoption-pref-id *<0-65535>*	A preference identifier for this radio port. The radio port is more likely to be adopted by a wireless switch that is its preferred wireless switch.
antenna-mode *<diversity|primary|secondary>*	Antenna diversity mode. You can select from the following options: • diversity–Full Diversity (both antennas). • primary–Primary Antenna only. • secondary–Secondary Antenna only. **NOTE** Before executing this command please ensure that the radio is present and is of type AP300.
beacon-interval*<50-200>*	Beacon interval in K-uSec.
bss (*<1-4>*|auto) WLAN	map wireless lans to radio bssids. • *<1-4>*–The bss where wireless lans will be mapped. • auto–Automatic assignment of bss. The user selects wireless lans, and the system assigns them to a bss automatically. • WLAN–A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices. When a bss is also specified, the first wlan will be used as the primary wlan. When the auto option is used, the system will automatically assign the first four wlans as primaries on their respective bss
cca-level*<1-31>*	CCA level value.
cca-mode*<0-3>*	CCA mode value.
channel-power (indoor|outdoor) (<1-2000>|acs|random) <4-20>	Location, channel and transmit power level. • indoor – Indoor location • outdoor – Outdoor location • *<1-2000>* – Channel number • acs – Auto channel selection (radio will scan for the least congested channel at startup or reconfiguration) • random – Random channel selection • *<4-20>* – Power in dBm

coordinates (X,Y,Z coordinates)	Configure the location of this radio in terms of x.y.z coordinates. • <-65535-65535> – X Coordinate • <-65535-65535> – Y Coordinate • <-65535-65535> – Z Coordinate
copy-config-from (<1-1000>|default-11a| default-11b|default-11bg)	Copy the configuration from a previously configured radio. • <1-1000> – A single radio index • default-11a – default 11a configuration template • default-11b – default 11b configuration template • default-11bg – default 11bg configuration template
description	Configure a description for this radio. Should not exceed 20 characters.
detector	Dedicate this radio as a detector. No mobile-units can associate to a detector.
dtim-period*<1-50>* bss *<1-4>*	DTIM period (number of beacons between successive DTIMs) `radio` **`dtim-period`***`<1-50>`* **`bss`***`<1-4>`* • *<1-50>* – DTIM period. • bss – *BSS* • *<1-4>* – BSS index
enforce-spec-mgmt (enable)	Enforce spectrum management checks on specified radios. Only mobile-units that advertise spectrum management capabilities will be allowed to associate on this radio
image-name	Image Name, shoyud not exceed more than 20 characters.
location-message	Specify message that would be sent to all mobile-units that associate with these radios. This message should not exceed more than 80 characters.
mac (AA-BB-CC-DD-EE-FF)	Change the parent (access-port) MAC address of the radio. • AA-BB-CC-DD-EE-FF – MAC address in AA-BB-CC-DD-EE-FF format.
max-mobile-units *<1-256>*	Maximum number of mobile-units allowed to associate.
on-channel-scan	Enable rogue scanning on this radio.

reset	reset a radio (this will only reset the specified radio, not the complete access-port)
reset-ap	reset the parent ap (this will reset all radios on that access-port)
rts-threshold*<0-2347>*	RTS threshold in bytes.
run-acs	Run auto-channel-selection on a radio. The radio should already have been configured for ACS
self-heal-offset *<0-30>*	Configure the self-healing offset, measured in dBm, for regulatory. **NOTE** This offset is based off the regulatory maximum power for the specified channel (the command "show wireless regulatory" shows the max power allowed)
short-preamble	Enable support for Short preamble **NOTE** This will disable support for long preamble and mobile-units that only support long preamble wont be able to associate.

speed	Configure the basic and supported data rates / speed. • 1 1-Mbps • 11 11-Mbps • 12 12-Mbps • 18 18-Mbps • 2 2-Mbps • 24 24-Mbps • 36 36-Mbps • 48 48-Mbps • 54 54-Mbps • 5p5 5.5-Mbps • 6 6-Mbps • 9 9-Mbps • basic1 basic 1-Mbps • basic11 basic 11-Mbps • basic12 basic 12-Mbps • basic18 basic 18-Mbps • basic2 basic 2-Mbps • basic24 basic 24-Mbps • basic36 basic 36-Mbps • basic48 basic 48-Mbps • basic54 basic 54-Mbps • basic5p5 basic 5.5-Mbps • basic6 basic 6-Mbps • basic9 basic 9-Mbps • default factory default rates based on radio-type • range all rates enabled, the lowest one set to basic • throughput all rates basic (note: only g clients allowed on 11bg radios)

wmm(background|best-effort|video|voice) (aifsn<*1-15*>|burst<*0-65535*>| cw<*0-15*>)	802.11e / Wireless MultiMedia (WMM) parameters (supported only on AP300). `radio wmm(background|best-effort|video|voice)(aifsn<1-15>|burst<0-65535>| cw<0-15>)` • background – background category traffic • best-effort– best effort category traffic • video –video traffic category traffic • voice – voice traffic category traffic • aifsn<*1-15*> – (Arbitration Inter Frame Spacing Number) The wait time in milliSeconds between data frames is derived using AIFSN and the slot-time. • burst<*0-65535*> – (transmit-opportunity) An interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium • cw<*0-15*> – (Contention Window parameters) wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window
add<*1-1000*> (MAC Address) (11a(ap300)| 11b(ap100|ap4131)| 11bg(ap300))	Add a new radio. `radio add<1-1000>(MAC Address)(11a(ap300)|11b(ap100|ap4131)|11bg(ap300))` • <1-1000> – Index where this radio is to be added • MAC – Mac address in AA-BB-CC-DD-EE-FF format • 11a – 802.11a type radio • 11b – 802.11b type radio • 11bg – 802.11bg type radio • ap300 – ap300 type access-port (default for 11a and 11bg) • ap100 – ap100 type access-port (default for 11b) • ap4131 – ap4131 type access-port

dns-name WORD (MAC Address)	Configure dns-name to be used in L3-Discovery on adopted access-ports. • AA-BB-CC-DD-EE-FF – Change the dns-name only on the access-port with a specified MAC address. If not specified, the dns-name update is sent to all currently adopted access-ports.

Usage Guidelines

Example

```
WS5100(config-wireless)#radio 250 bss auto 3-5
WS5100(config-wireless)#
```

17.1.23 self-heal

Wireless Configuration Commands

Use this CLI command to configure Self Healing.

Syntax

```
self-heal(interference-avoidance|neighbor-recovery)

self-heal interference-avoidance(enable|hold-time<0-65535>|
retries<0.0-15.0>)

self-heal neighbor-recovery(action|enable|neighbors|run-neighbor-detect)
self-heal neighbor-recovery action(both|none|open-rates|raise-power)
radio(<1-1000>|RADIO)
self-heal neighbor-recovery neighbors<1-1000>(<1-1000>|RADIO)
```

Parameters

interference-avoidance	Interference Avoidance configuration
enable	enable/disable interference avoidance
hold-time<*0-65535*>	The number of seconds to disable interference avoidance after a detection . This prevents a radio from changing channels continuously.Set the hold-time between 0-65535 seconds.
retries<*0.0-15.0*>	The average number retries to cause a radio to re-run auto channel selection. Set a value between 0-15.
neighbor-recovery	Neighbor Recovery configuration commands
action (both|none|open-rates| raise-power) radio (<*1-1000*>|RADIO)	Radio self healing action when neighbors are detected down. • both – raise the power to max and open all rates. • none – do nothing. • open-rates – open all rates. • raise-power – raise the power to max. • **radio** – modify the action for specified radio(s). • <*1-1000*> – A single radio index. • RADIO – A list (eg: 1,3,7) or range (eg: 3-7) of radio indices.
enable	Monitor access-ports and attempt to increase coverage on failure.

neighbors*<1-1000>* (<1-1000>|RADIO)	Add radios as neigbors.
run-neighbor-detect	Disassociate all mobile-units, clear current neigbors and run neighbor detection.

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

17.1.24 sensor

Wireless Configuration Commands

Use this CLI command to configure Wireless Intrusion Protection System parameters.

Syntax

```
sensor(default-config|vlan)
sensor default-config(ip-mode|wips-server-ip)
sensor default-config ip-mode(dhcp|static(A.B.C.D/M)(A.B.C.D))
sensor default-config wips-server-ip(primary|secondary)(A.B.C.D)
```

Parameters

default-config	default configuration sent to sensors when they are configured.
ip-mode	configure the IP address mode of the sensors.
dhcp	sensor should use DHCP to obtain an IP address.
static (A.B.C.D/M)(A.B.C.D)	sensor must use the specific static IP address. • A.B.C.D/M – sensor IP address and network mask • A.B.C.D – specify the gateway IP address for sensors
wips-server-ip	specify IP addresses of the WIPS server.
primary (A.B.C.D)	specify the primary IP address of the WIPS server.
secondary (A.B.C.D)	specify the seconary IP address of the WIPS server
vlan*<1-4094>*	Configure vlans where sensors are to be discovered.

Usage Guidelines

Example

```
WS5100(config-wireless)#sensor vlan 268 500
WS5100(config-wireless)#
```

17.1.25 service

Wireless Configuration Commands

Use this CLI command to invoke the service commands to trobuleshoot or debug the `(config-wireless)` instance configurations.

Syntax

```
service(ap|clear|diag-shell|save-cli|show|
start-shell|tethereal|wireless)

service ap(force-dump))
service clear(all|cores|dumps|panics)

service show(ap|cli|command-history|crash-info|info|last-passwd|reboot-
history|startup-log|upgrade-history|wireless)
service show ap beacon-count
```

Parameters

ap	access-port serviceability parameters.
force-dump	trigger the access-port to send a crash-dump to the wireless-switch.
clear	Remove specified support information
all	Remove all core, dump and panic files
cores	Remove all core files
dumps	Remove all dump files
panics	Remove all kernel panic files
diag-shell	Provide diag shell access.
save-cli	Save CLI tree for all modes in html format.
show	Show running system information.
start-shell	Provide shell access.
tethereal	Dump and analyze network traffic.
wireless	Wireless parameters.

Usage Guidelines

Example

```
WS5100(config-wireless)#service clear all
WS5100(config-wireless)#

WS5100(config-wireless)#service clear cores
WS5100(config-wireless)#

WS5100(config-wireless)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
WS5100(config-wireless)#

WS5100(config-wireless)#service show ?
  ap               access-port serviceability parameters
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history
  wireless         Wireless parameters
WS5100(config-wireless)#

WS5100(config-wireless)#service show info
4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.4M out of 18.6M available for crashinfo.
List of Files:
messages.log                    0       Oct 3  13:43
snmpd.log                       316     Oct 3  13:43
startup.log                     16.6k   Oct 3  13:43
command.history                 2.0k    Oct 7  02:24
reboot.history                  3.3k    Oct 3  13:43
upgrade.history                 782     Aug 29 18:32
Please export these files or delete them for more space.
WS5100(config-wireless)#

WS5100(config-wireless)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:
WS5100(config-wireless)#
```

```
WS5100(config-wireless)#service tethereal ?
  LINE  tethereal options in the format
        [-V (print detailed packet)] [-x (hex dump of packet)]
        [-p (no promiscuous mode for interface)]
        [-n (disable name resolution)] [-c <count> ] [-h (detailed help)]
        [-E (to capture ESPD) ][-e (capture nonEspd packets)]
        [-f <capture filter expression in format "xx xx xx"> ]
        [-i <interface on which to capture packets> ] [-W (wisp packet
only)]
        [-s <snaplen> ] [-r <filename> (read contents of specified file)]
        [-w <savefile> (save capture in specified file) ]
        [-X (for examples on tethereal capture filter) ]

WS5100(config-wireless)#service tethereal

WS5100(config-wireless)#service wireless ?
  dump-core         Create a core file of the ccsrvr process
  dump-state        Create a ccsrvr.dump file in nvram with internal state
                    information
  mu-history        Enable mu association history
  mu-history-clear  Delete all mu association history files
  rate-scale        Enable wireless rate scaling (default)
  request-ap-log    Request ap Log

WS5100(config-wireless)#service wireless
```

17.1.26 show

Wireless Configuration Commands

Use thie CLI command to view the current system information that is running on the WS5100 Series Wirteless Switch.

Syntax

```
show<paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

Example

```
WS5100(config-wireless)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
```

```
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

WS5100(config-wireless)#show
```

17.1.27 smart-scan-channels

Wireless Configuration Commands

Use this CLI command to configure a list of channels that are used on the network. This list will be provided to mobile-units that can support partial scanning.

Syntax

```
smart-scan-channels(11a|11bg)<1-200>
```

Parameters

11a	Specify channel list for the 5Ghz band used by 802.11a mobile-units.
11bg	Specify channel list for the 2.4Ghz band used by 802.11bg mobile-units.
<1-200>	List of channels.

Usage Guidelines

Example

```
EXAMPLE OUTPUT HERE
```

17.1.28 terminal

Wireless Configuration Commands

Use this command to set the length /number of lines to be displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copy debug output to the current terminal line
no	Negate a command or set its defaults

Usage Guidelines

Example

```
WS5100(config-wireless)#terminal monitor
WS5100(config-wireless)#

WS5100(config-wireless)#terminal no monitor
WS5100(config-wireless)#
```

17.1.29 wlan

Wireless Configuration Commands

Use this CLI command to confiugure Wireless LAN related commands.

Syntax

```
wlan(<1-32>|WLAN)
(accounting|answer-bcast-ess|authentication-type| description
|dot11i|enable|encryption-type|hotspot|inactivity-timeout|kdc|mobility|
mu-mu-disallow|qos|radius|secure-beacon|ssid|symbol-extensions
|syslog|tunnel|vlan|wep128|wep64)

wlan<1-32>(none|radius|ssyslog)
wlan<1-32> authentication-type(eap|hotspot|kerberos|mac-auth|none)

wlan<1-32> dot11i(handshake|key|key-rotation|key-rotation-interval|
opp-pmk-caching|phrase|pmk-caching|preauthentication|second-key|
tkip-cntrmeas-hold-time)
wlan<1-32> dot11i handshake timeout<100-5000> retransmit<1-10>
wlan<1-32> key(0|2|WORD)

wlan<1-32> encryption-type(ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep128-keyguard|wep64)

wlan<1-32> hotspot(allow-list|webpage|webpage-location)
wlan<1-32> hotspot allow-list(Rule index)(IP address)
wlan<1-32> hotspot webpage(external|internal)(failure|login|welcome)
wlan<1-32> hotspot webpage-location(advanced|external|internal)

wlan<1-32>
kdc(password(0||LINE)|realm(LINE)|server(primary|secondary|timeout))
wlan<1-32> kdc server (primary|secondary|timeout)auth-port<1-65535>

wlan<1-32> qos(classification|mcast1|mcast2|prioritize-voice|svp|wmm)
wlan<1-32> qos classification(background|best-effort|video|voice|wmm)
wlan<1-32> qos wmm(8021p|background|best-effort|dscp|video|voice)
(aifsn|cw|txop-limit|acm)

wlan<1-32> radius(accounting|authentication-protocol|dscp|
dynamic-authorization|dynamic-vlan-assignment|mobile-unit|reauth|server)

wlan<1-32> radius accounting(mode|timeout)
wlan<1-32> radius accounting mode(start-interim-stop(interval)
<60-3600>|start-stop|stop-only|)
wlan<1-32> radius accounting timeout<1-60> retransmit<1-100>

wlan<1-32> radius authentication-protocol(chap|pap)
```

```
wlan<1-32> radius server(primary|secondary|timeout)
wlan<1-32> radius server(primary|secondary)
(ip-address(auth-port)<1024-65535>)(radius-key(0|2|LINE))
wlan<1-32> radius server timeout<1-60> retransmit<1-10>

wlan<1-32> syslog (accounting) server<IP Address> port<Port Number>

wlan<1-32> tunnel<1-32> gateway<IP Address and mask>

wlan<1-32> wep128(key<1-4> (ascii|hex[0|2|WORD])|phrase(LINE)|
wep-default-key<1-4>)
```

Parameters

<1-32>	A single wlan index.
WLAN	A list (eg: 1,3,7) or range (eg: 3-7) of wlan indices.
accounting (none|radius|syslog)	Accounting on this WLAN. • none – No accounting on this WLAN • radius – Use RADIUS accounting on this WLAN • syslog – Use Syslog accounting on this WLAN
answer-bcast-ess	Allow this WLAN to respond to probes for broadcast ESS.
authentication-type (eap|hotspot|kerberos| mac-auth|none)	The authentication type of this WLAN. • eap – EAP authentication (802.1X) • hotspot – Web based authentication • kerberos – Kerberos authentication (Note: encryption type will change to wep128 if its not already wep128/keyguard) • mac-auth – MAC authentication (Radius lookup of MAC address) • none – None / pre-shared keys
description	The description of this WLAN
dot11i ()	Modify tkip/ccmp (802.11i) related parameters

handshake timeout*<100-5000>* retransmit*<1-10>*	Use handshake to configure the timeout and retransmission. • timeout*<100-5000>* – The timeout in milliseconds, between retries. • retransmit*<1-10>* – The number of retransmission attempts.
key(0|2|WORD)	Configure the key (PMK). • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • WORD – The 256bit (64 hex characters) long key.
key-rotation(enable)	Control the periodic update of the broadcast keys of all associated mobile-units.
key-rotation-interval *<1800-86400>*	Configure the broadcast key rotation interval.
opp-pmk-caching	Enable the opportunistic use of cached pairwise master keys (fast roaming with eap/802.1X).
phrase(0|2|LINE)	Configure the passphrase. • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • LINE – A passphrase between 8 and 63 characters long.
pmk-caching	Enable the use of cached pairwise master keys (fast roaming with eap/802.1X).
preauthentication	Enable support for 802.11i preauthentication.
second-key(enable|key|phrase) (0|2|WORD)	Configure a secondary set of key/passphrase for this wlan. • enable – Enable the use of a secondary key/passphrase. • key – Configure the key (PMK). • phrase – Configure the passphrase. • 0 – Password is specified UNENCRYPTED • 2 – Password is encrypted with password-encryption secret • WORD – The 256bit (64 hex characters) long key

tkip-cntrmeas-hold-time *<0-65535>*	Configure the hold-time in seconds for which clients are blocked when tkip countermeasures are taken.Default is 60 seconds.
enable()	enable specified wireless lan(s).
encryption-type()	The encryption type for this WLAN.
ccmp	AES Counter Mode CBC-MAC Protocol (AES-CCM/CCMP)
keyguard	Keyguard-MCM (Mobile Computing Mode)
none	no encryption
tkip	Enable Temporal Key Integrity Protocol (TKIP)
tkip-ccmp	Enable both tkip and ccmp on this WLAN
wep128	Enable Wired Equivalence Privacy (WEP) with 128 bit keys
wep128-keyguard	Enable both WEP128 as well as Keyguard-MCM on this WLAN
wep64	Enable Wired Equivalence Privacy (WEP) with 64 bit keys. **NOTE** A configuration where two WLANs are mapped to the same VLAN, and one of them is configured with no encryption and the other with WEP, is insecure. It can lead to a compromise of the WEP key.
hotspot()	Modify hotspot related parameters.
allow (Rule index) (IP address)	Modify hotspot allow-list parameters. Users who have not yet authenticated will be allowed access to these IP addresses. • Rule index – Allow-list Rule index. Should be between (1-10). • IP address – allow-list IP address

webpage(external|internal) (failure|login|welcome)	Modify hotspot page parameters. • external – Modify hotspot External page. • internal – Modify hotspot Internal page. • failure – Users are redirected to this webpage if they fail authentication. • login – Users are prompted for their username and password on this webpage. • welcome – Users are redirected to this webpage after they authenticate successfully.
webpage-location (advanced|external| internal)	The location of the webpages to be used for authentication. These pages can either be hosted on the wireless switch or on an external web server. • advanced – use login/welcome/failure web pages created by the user on the wireless switch. • external – use login/welcome/failure web pages on an external server. • internal – use login/welcome/failure web pages created automatically on the wireless switch.
inactivity-timeout *<60-86400>*	Inactivity timeout in seconds. If a frame is not received from a mobile-unit for this amount of time, the mobile-unit is disassociated.
kdc()	Modify KDC related parameters.
password(0|2|LINE)	Kdc server password, upto 127 characters. • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • LINE – Kdc server password, upto 127 characters.
realm(LINE)	Kdc realm 127 characters. • LINE – Kdc realm, upto 127 characters.

server (primary|secondary) (IP address) auth-port *<1-65535>*	Modify KDC server parameters. • primary – Primary kdc server • secondary – Secondary kdc server • IP address – Kdc server IP address • auth-port*<1-65535>* – Kdc server authentication port. Default is 88.
server(timeout)*<1-60>*	Modify KDC server parameters. • timeout – Time the wireless switch waits for a response from the kdc server before retrying.
mobility (enable)	Enable L3 Mobility on WLAN(s).
mu-mu-disallow (switch-to-wired)	Disallow frames from one mu to another mu on this WLAN. • switch-to-wired – Disallow by switching the frame out on the wired side (to allow an externalswitch to decide whether this frame is to be allowed or dropped)
qos()	Quality of Service commands.
classification (background|best-effort|video|voice|wmm)	Select how traffic on this WLAN must be classified (relative prioritization on the access-port). • background – All traffic on this wlan is treated as background traffic. • best-effort – All traffic on this wlan is treated as Best-Effort. • video – All traffic on this wlan is treated as Video. • voice – All traffic on this wlan is treated as Voice. • wmm – Use WMM based classification, using DSCP or 802.1p tags to classify traffic into different queues.
mcast1|mcast2 (AA-BB-CC-DD-EE-FF)	The Egress prioritization multicast mask. • AA-BB-CC-DD-EE-FF – Mac address in AA-BB-CC-DD-EE-FF format.
prioritize-voice	Prioritize voice frames over general data frames (applies non-WMM mobile-unit)
svp(enable)	Enable Spectralink Voice Prioritization support on this WLAN.

wmm (8021p|background| best-effort| dscp|video|voice) (aifsn|cw|txop-limit|acm)	802.11e / Wireless MultiMedia (WMM) parameters (supported only on AP300). • 8021p – Use 802.1p frame priority (field in the VLAN tag) to determine packet priority. • background – background category traffic. • best-effort – best effort category traffic. • dscp – Use DSCP (Differentiated Services Code Point) bits in the IP header to determine packet priority. • video – video traffic category traffic. • voice – voice traffic category traffic. • aifsn – (Arbitration Inter Frame Spacing Number) the wait time in milliSeconds between data frames is derived using AIFSN and the slot-time. • cw – (Contention Window parameters): wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmission. Stations then double their wait time on a collision, until it reaches the maximum contention window • txop-limit – (transmit-opportunity): an interval of time when a particular WMM STA has the right to initiate transmissions onto the wireless medium. • acm – admission control parameters

radius (accounting| authentication-protocol| dscpdynamic-authorization| dynamic-vlan-assignment| mobile-unit|reauth|server)	Modify Radius/802.1X related parameters. • accounting – Accounting Parameters • authentication-protocol – Authentication protocol to use in the radius requests • dscp – Specify a DSCP (Differentiated Services Code Point) value to provide QoS to Radius packets. • dynamic-authorization – Configure support for Radius dynamic authorization extensions such as Disconnect Message, and Change-Of-Authorization, as described in RFC 3576. • dynamic-vlan-assignment – Allow users to be assigned to Radius server specified VLANs, instead of only the vlan that is mapped to this wlan. • mobile-unit – Modify Radius/802.1X supplicant related parameters. • reauth – Enable periodic reauthentication of all associated mobile-units. • server – Modify Radius/802.1X server parameters.
accounting mode(start-interim-stop(interval)<60-3600>|start-stop|stop-only)	Use this to configure the radius accounting parameters. • **mode** – Accounting Mode on this WLAN • start-interim-stop – Accounting Start-Interim-Stop • **interval***<60-3600>* – Time Interval between successive accounting updates. • start-stop – Send Accounting Start-Stop • stop-only – Send Accounting Stop only
accounting timeout*<1-60>* retransmit*<1-100>*	Use this to configure the radius accounting parameters. • timeout *<1-60>* – Time in seconds that the wireless switch waits for a response from the radius server before retrying Accounting. • **retransmit** *<1-100>* – Number of retries before the wireless switch will give up Accounting.

authentication-protocol (chap|pap)	Authentication protocol to use in the radius requests. • chap – Challenge Handshake Authentication Protocol • pap – Password Authentication Protocol
dscp*<0-63>*	Specify a DSCP (Differentiated Services Code Point) value to provide QoS to Radius packets.The DSCP value should be between 0-63.
dynamic-authorization (enable)	Configure support for Radius dynamic authorization extensions such as Disconnect Message, and Change-Of-Authorization, as described in RFC 3576. • enable – Enable support for Radius dynamic authorization.
dynamic-vlan-assignment	Allow users to be assigned to Radius server specified VLANs, instead of only the vlan that is mapped to this wlan. • enable – Enable dynamic/radius-assigned vlan assignment.
mobile-unit **timeout***<1-60>* **retransmit***<1-10>*	Modify Radius/802.1X supplicant related parameters. • timeout<1-60> – Time in seconds that the wireless switch waits for a response from the mobile-unit before retrying • retransmit<1-10> – Number of retries before the wireless switch will give up and disassociate the mobile-unit.
reauth*<30-65535>*	Enable periodic reauthentication of all associated mobile-units. • *<30-65535>* – Reauthentication period in seconds.
server(primary|secondary) (ip-address **(auth-port)** *<1024-65535>*) (radius-key(0|2|LINE))	Modify Radius/802.1X server parameters. • primary – Primary radius server • secondary – Secondary radius server • ip-address – Radius server IP address • auth-port*<1024-65535>* – Radius server authentication port (default:1812) • radius-key – Radius server shared secret, upto 127 characters • 0 – Password is specified UNENCRYPTED • 2 – Password is encrypted with password-encryption secret • LINE – Radius server shared secret, upto 127 characters

server **timeout***<1-60>* **retransmit***<1-10>*	Modify Radius/802.1X server parameters. • timeout*<1-60>* – Time, in seconds, the wireless switch waits for a response from the radius server before retrying. • retransmit*<1-10>* – Number of retries before the wireless switch will give up and disassociate the mobile-unit.
secure-beacon	dont include the SSID of this WLAN in Beacon frames.
ssid	The SSID of this WLAN.
symbol-extensions fast-roaming (enable)	Enable support for Symbol extensions • fast-roaming(enable) – Enable support for Symbol fast roaming.
syslog (accounting) server <IP Address> port <Port number>	Syslog Accounting. • accounting – Modify Accounting Parameters • server<IP Address> – Modify Syslog Accounting Server IP Address. • port <Port Number> – Syslog Server Port. Default port number is 514.
tunnel*<1-32>* gateway <IP Address and mask>	• tunnel<1-32> – The tunnel index mapping for this WLAN • gateway <IP address> – The gateway IP address and mask
vlan*<1-4094>*	The VLAN assignment of this WLAN.

wep128 (key*<1-4>* (ascii|hex)<0|2|WORD> | phrase(LINE) | wep-default-key*<1-4>)*	Configure WEP128 parameters. • key*<1-4>* – configure pre-shared hex keys • ascii – keys as ascii characters (5 characters for wep64, 13 for wep128) • hex – keys as hexadecimal characters (10 characters for wep64, 26 for wep128) • 0 – Password is specified UNENCRYPTED • 2 – Password is encrypted with password-encryption secret • WORD – Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128) • phrase – Specify a passphrase from which the keys are to be derived • LINE – the passphrase (between 4 and 32 characters) • wep-defauly-key*<1-4>* – The key index to be used for transmission from AP to MU
wep64	Configure WEP64 parameters.

Usage Guidelines

Example

```
WS5100(config-wireless)#wlan 25 accounting syslog
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 answer-bcast-ess
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 authentication-type kerberos
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 description "TestWLAN"
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 dot11i handshake timeout 2500 retransmit 5
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 dot11i key-rotation enable
WS5100(config-wireless)#
```

```
WS5100(config-wireless)#wlan 25 dot11i key-rotation-interval 2000
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 enable
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 hotspot webpage external failure "This
feature is under development"
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 kdc server primary 1.2.3.4 auth-port 50000
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 mobility enable
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 radius accounting timeout 30 retransmit 50
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 radius mobile-unit timeout 30 retransmit 5
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 ssid TestString
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 symbol-extensions fast-roaming enable
WS5100(config-wireless)#

WS5100(config-wireless)#wlan 25 syslog accounting server 12.13.14.125 port
5005
WS5100(config-wireless)#
```

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, New York 11742-1300
http://www.symbol.com

72E-85974-01
Revision A October 2006